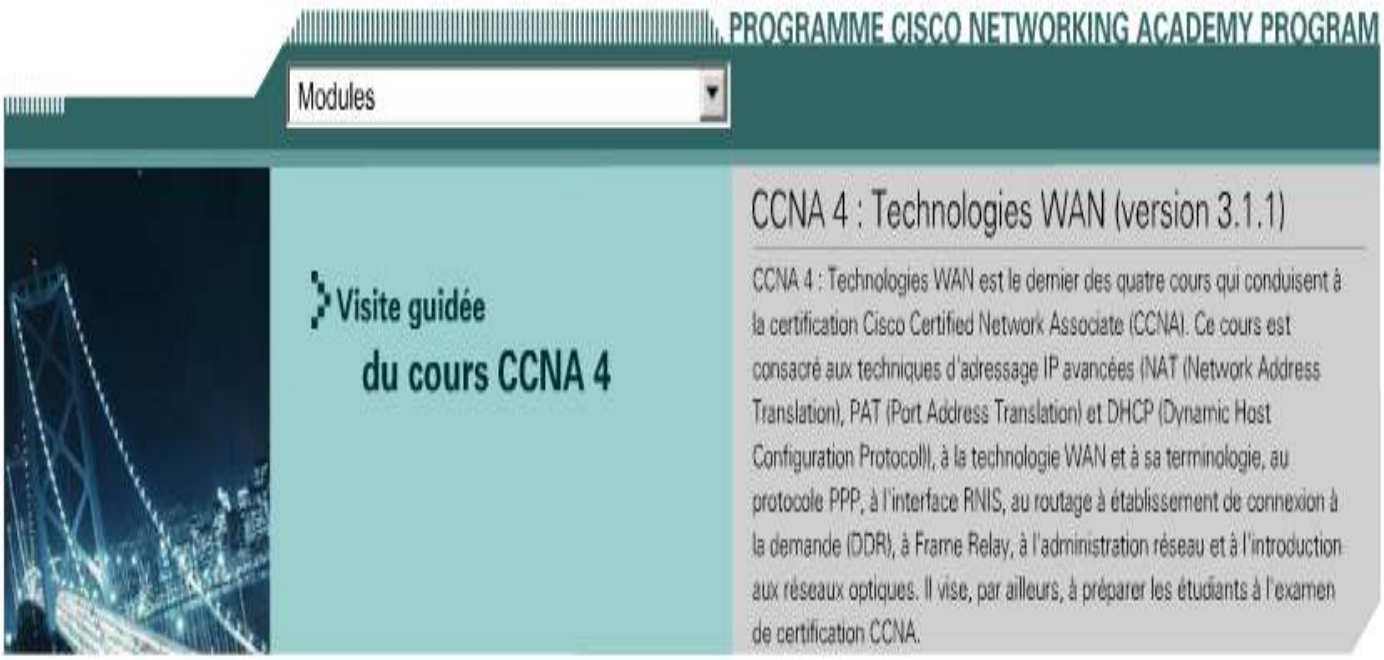
Ce livre à été télécharger à www.phpmaroc.com
Rassembler à partir de:
www.cisco.com


PROGRAMME CISCO NETWORKING ACADEMY PROGRAM
Modules
Visite guidée
du cours CCNA 4
CCNA 4 : Technologies WAN (version 3.1.1)
CCNA 4 : Technologies WAN est le dernier des quatre cours qui conduisent à la certification Cisco Certified Network Associate (CCNA). Ce cours est consacré aux techniques d'adressage IP avancées (NAT (Network Address Translation), PAT (Port Address Translation) et DHCP (Dynamic Host Configuration Protocol)), à la technologie WAN et à sa terminologie, au protocole PPP, à l'interface RNIS, au routage à établissement de connexion à la demande (DDR), à Frame Relay, à l'administration réseau et à l'introduction aux réseaux optiques. Il vise, par ailleurs, à préparer les étudiants à l'examen de certification CCNA.

Les logos et marques cités dans ce document sont la propriété de leurs auteurs respectifs
Copyright :
Ce tutorial est mis à disposition gratuitement au format HTML lisible en ligne par son auteur sur le site http://www.cisco.com, son auteur préserve néanmoins tous ses droits de propriété intellectuelle.
Ce tutorial ne saurait être vendu, commercialisé, offert à titre gracieux, seul ou packagé, sous quelque forme que ce soit par une personne autre que son auteur sous peine de poursuite judiciaire.
L'auteur ne pourra pas être tenu responsable pour les dommages matériel ou immatériel, perte d'exploitation ou de clientèle liés à l'utilisation de ce tutorial.

Vue d'ensemble

La croissance rapide d'Internet a surpris la plupart des observateurs. Cette croissance est notamment due à la souplesse de la conception originale. Sans le développement de nouvelles méthodologies d'assignation d'adresses IP, cette croissance rapide aurait épuisé la réserve existante d'adresses IP. Pour pallier à cette pénurie d'adresses IP, plusieurs solutions ont été développées. L'une de ces solutions, largement mise en oeuvre, est la traduction d'adresses réseau (NAT).

NAT est un mécanisme permettant de conserver les adresses IP enregistrées dans des réseaux de grande taille et de simplifier la gestion de l'adressage IP. Lorsqu'un paquet est routé par un équipement de réseau, généralement un pare-feu ou un routeur périphérique, l'adresse IP source, c'est à dire une adresse réseau interne privée, est traduite en une adresse IP publique routable. Cela permet de transporter le paquet sur des réseaux externes publics, tels qu'Internet. L'adresse publique de la réponse est ensuite retraduite en une adresse interne privée pour être livrée sur le réseau interne. Une variation de NAT, dénommée PAT (*Port Address Translation* - Traduction d'adresses de ports), permet de traduire un grand nombre d'adresses privées internes au moyen d'une adresse publique externe unique.

Les routeurs, les serveurs et les autres équipements primordiaux du réseau nécessitent généralement une configuration IP statique, saisie manuellement. En revanche, les ordinateurs de bureau clients n'ont pas besoin d'une adresse spécifique, mais plutôt d'une adresse quelconque prise dans une série. Cette série appartient généralement à un sous-réseau IP. Une station de travail d'un sous-réseau spécifique peut recevoir n'importe quelle adresse dans une plage, alors que d'autres valeurs sont statiques, notamment le masque de sous-réseau, la passerelle par défaut et le serveur DNS.

Le protocole DHCP (*Dynamic Host Configuration Protocol*) a été conçu pour attribuer de façon dynamique les adresses IP et d'autres informations importantes de configuration réseau. Comme les machines de bureau clientes constituent la plupart des nœuds du réseau, DHCP offre un gain de temps extrêmement utile aux administrateurs réseau.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Identifier les adresses IP privées décrites dans la RFC 1918
- Discuter des caractéristiques des fonctions NAT et PAT
- Expliquer les avantages offerts par NAT
- Expliquer comment configurer les fonctions NAT et PAT, notamment la traduction statique, la traduction dynamique et la surcharge
- Identifier les commandes utilisées pour vérifier la configuration des fonctions NAT et PAT
- Énumérer les étapes utilisées pour dépanner la configuration des fonctions NAT et PAT
- Discuter des avantages et des inconvénients de NAT
- Décrire les caractéristiques du protocole DHCP
- Expliquer les différences entre les protocoles BOOTP et DHCP
- Expliquer le processus de configuration de clients DHCP
- Configurer un serveur DHCP
- Vérifier le fonctionnement du protocole DHCP
- Dépanner une configuration DHCP
- Expliquer les requêtes de relais DHCP

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
1.1	Évolutivité des réseaux avec la traduction d'adresses réseau (NAT) et la traduction d'adresses de ports (PAT)
1.2	Protocole DHCP (Dynamic Host Configuration Protocol)

1.1 Évolutivité des réseaux avec NAT et PAT

1.1.1 Adresses privées

La RFC 1918 réserve les trois blocs d'adresses IP privées ci-dessous:

- 1 adresse de classe A
- 16 adresses de classe B
- 256 adresses de classe C [1]

Classe	Plage d'adresses internes RFC 1918	Préfixe CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

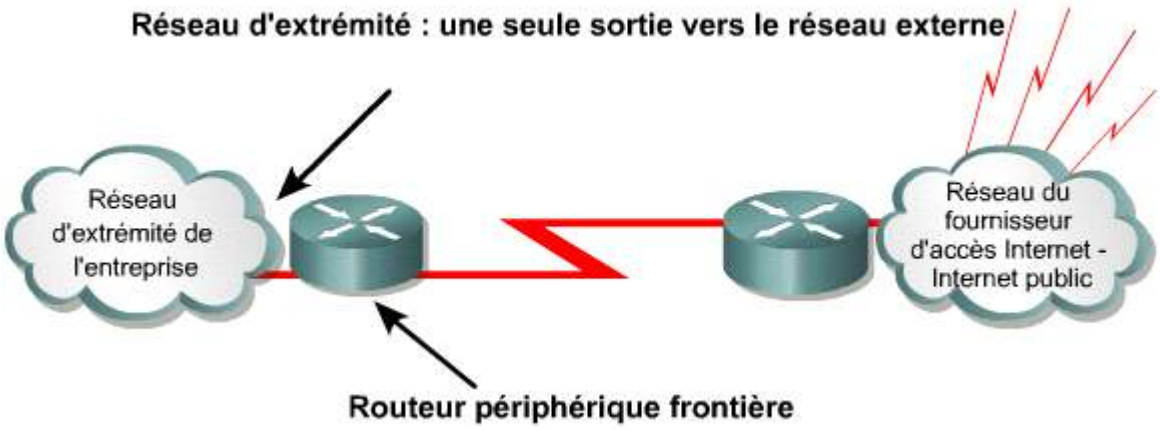
Ces adresses sont exclusivement destinées aux réseaux internes privés. Les paquets qui les contiennent ne sont pas routés sur Internet.

Les adresses Internet publiques doivent être enregistrées par une société faisant autorité sur Internet, par exemple l'ARIN (*American Registry for Internet Numbers*) ou le RIPE (*Réseaux IP Européens*), le registre Internet régional responsable de l'Europe et de l'Afrique du Nord. Ces adresses Internet publiques peuvent également être concédées par un FAI. Les adresses IP privées sont réservées et peuvent être utilisées par n'importe qui. Cela signifie que deux réseaux ou deux millions de réseaux peuvent chacun utiliser la même adresse privée. Un routeur ne doit jamais router d'adresses RFC 1918. En effet, les FAI configurent généralement les routeurs périphériques de façon à empêcher le transfert du trafic privé. La fonction NAT offre de grands avantages aux sociétés individuelles et à Internet. Avant NAT, un hôte doté d'une adresse privée ne pouvait pas accéder à Internet. Avec NAT, les sociétés individuelles peuvent attribuer des adresses privées à certains ou tous leurs hôtes, et utiliser NAT pour leur procurer un accès à Internet.

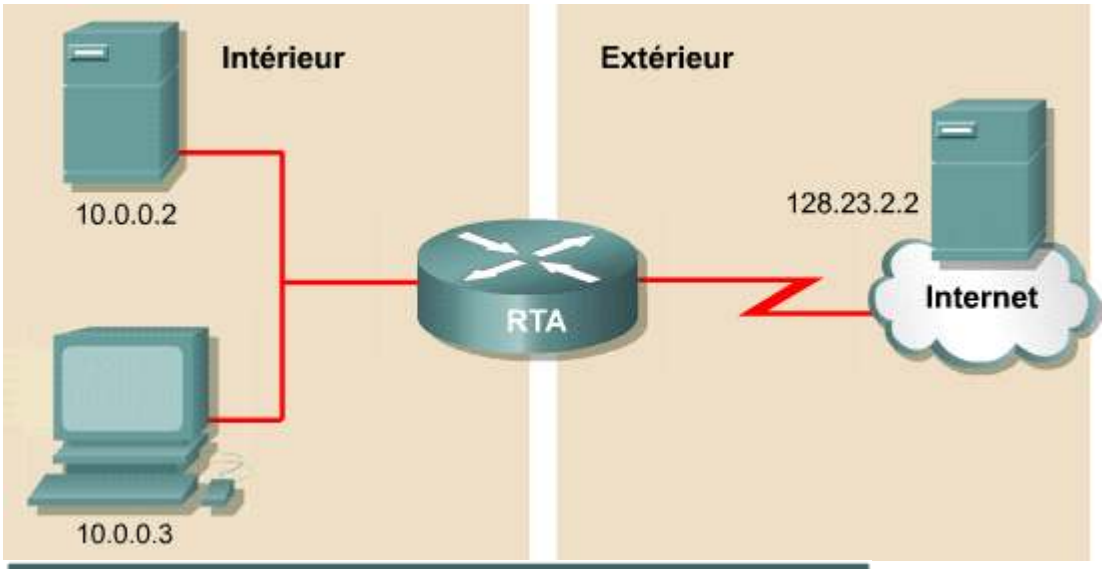
1.1 Évolutivité des réseaux avec NAT et PAT

1.1.2 Présentation des fonctions NAT et PAT

NAT est conçu pour conserver des adresses IP et permettre aux réseaux d'utiliser des adresses IP privées sur les réseaux internes. Ces adresses internes privées sont traduites en adresses publiques routables. Pour ce faire, des équipements d'interréseau utilisent des logiciels NAT spécialisés qui peuvent rendre le réseau moins vulnérable en masquant les adresses IP internes. Un matériel compatible NAT fonctionne généralement à la périphérie d'un réseau d'extrémité. Un réseau d'extrémité est un réseau ayant une connexion unique vers son réseau voisin. [1]


Réseau d'extrémité : une seule sortie vers le réseau externe
Réseau d'extrémité de l'entreprise
Réseau du fournisseur d'accès Internet - Internet public
Routeur périphérique frontière

Quand un hôte situé à l'intérieur du réseau d'extrémité souhaite émettre vers un hôte de l'extérieur, il transfère le paquet au routeur périphérique frontière. Ce routeur périphérique frontière effectue le processus NAT et traduit l'adresse privée interne d'un hôte en une adresse publique externe routable. [2]



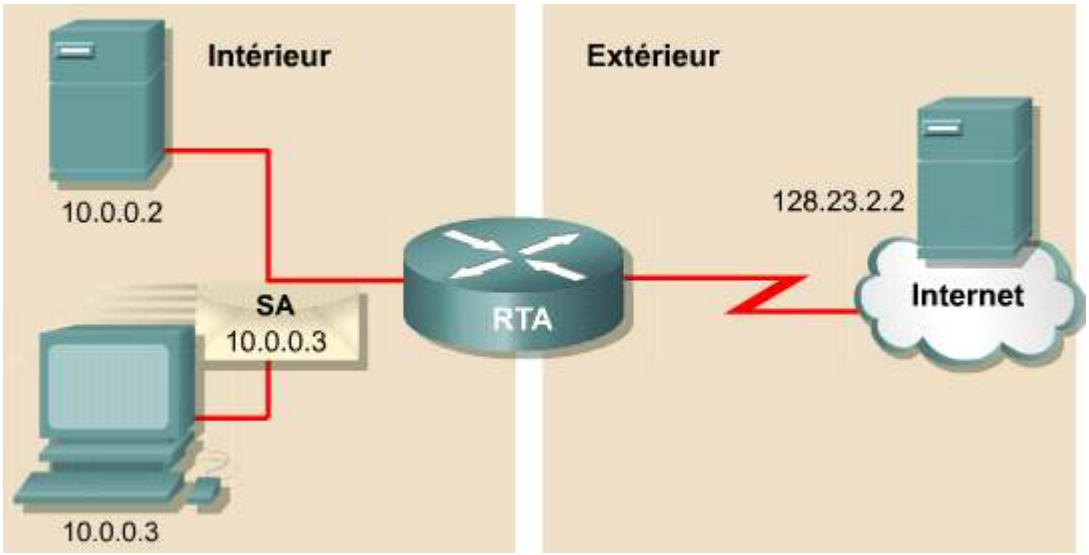
Fenêtre contextuelle (pop up)

Un hôte interne (10.0.0.3) veut communiquer avec un hôte externe (128.23.2.2). L'hôte interne envoie un paquet à la passerelle, RTA.

RTA détermine que le paquet doit être routé en externe, vers Internet. Le processus NAT choisit une adresse IP globalement unique (179.9.8.80) et remplace l'adresse locale du champ source du paquet par l'adresse globale. Il stocke ce mappage de l'adresse locale sur l'adresse globale dans la table NAT.

Le paquet est routé vers sa destination. Dans cet environnement client-serveur, le serveur peut répondre par un paquet, qui revient à RTA, adressé à l'adresse globale 179.9.8.80.

Le processus NAT détermine qu'un paquet est routé de l'extérieur vers l'intérieur et consulte la table NAT pour y trouver le mappage de cette adresse globale en une adresse locale. S'il trouve un mappage, l'adresse globale du champ de destination du paquet est remplacée par l'adresse locale et le paquet est transféré en interne.



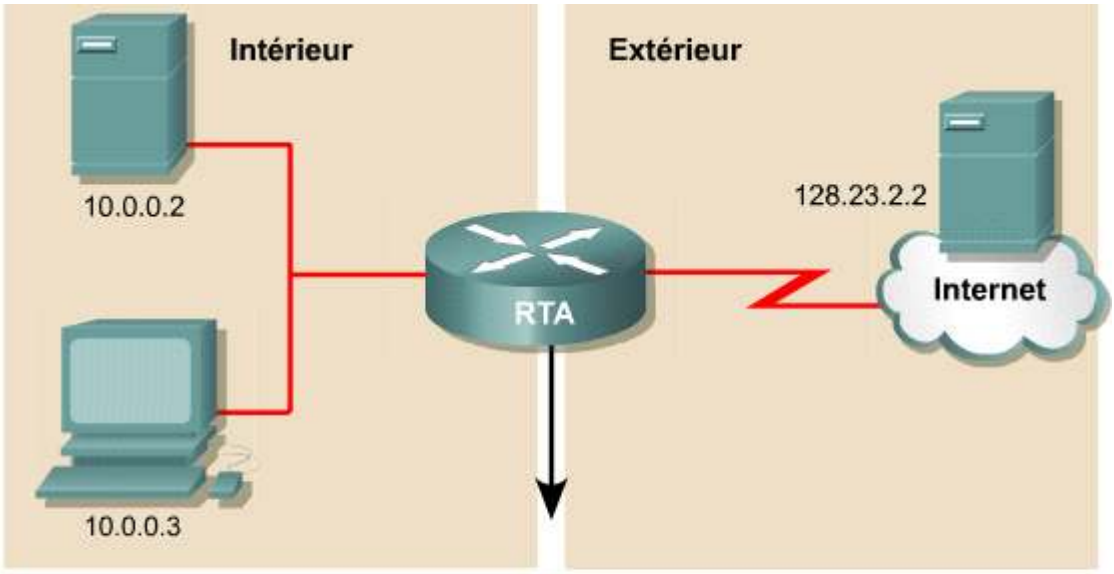
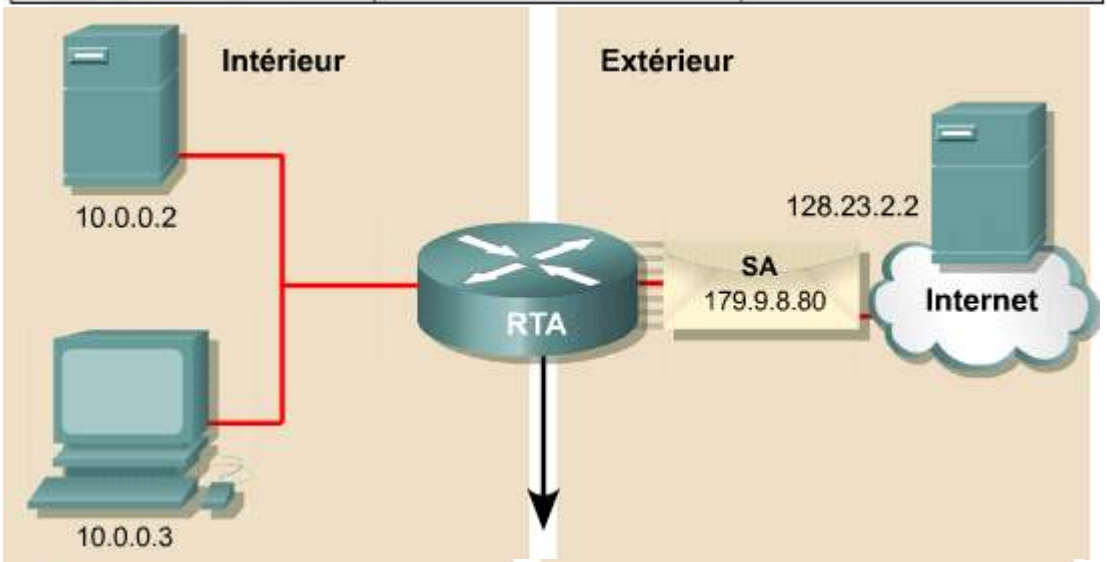
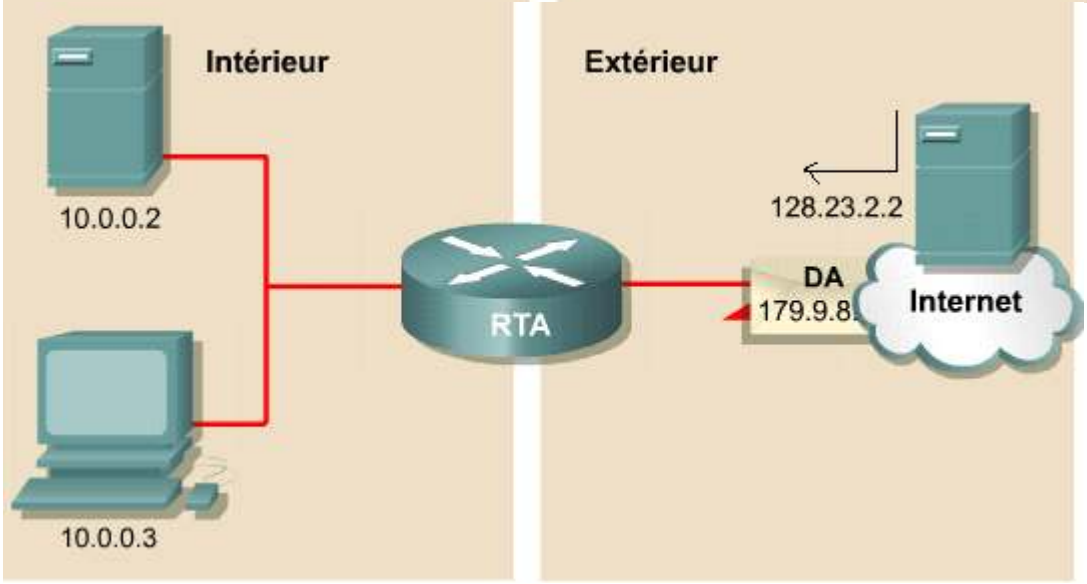


Table NAT		
Adresse IP locale interne	Adresse IP globale interne	Adresse IP globale externe
10.0.0.3	179.9.8.80	128.23.2.2





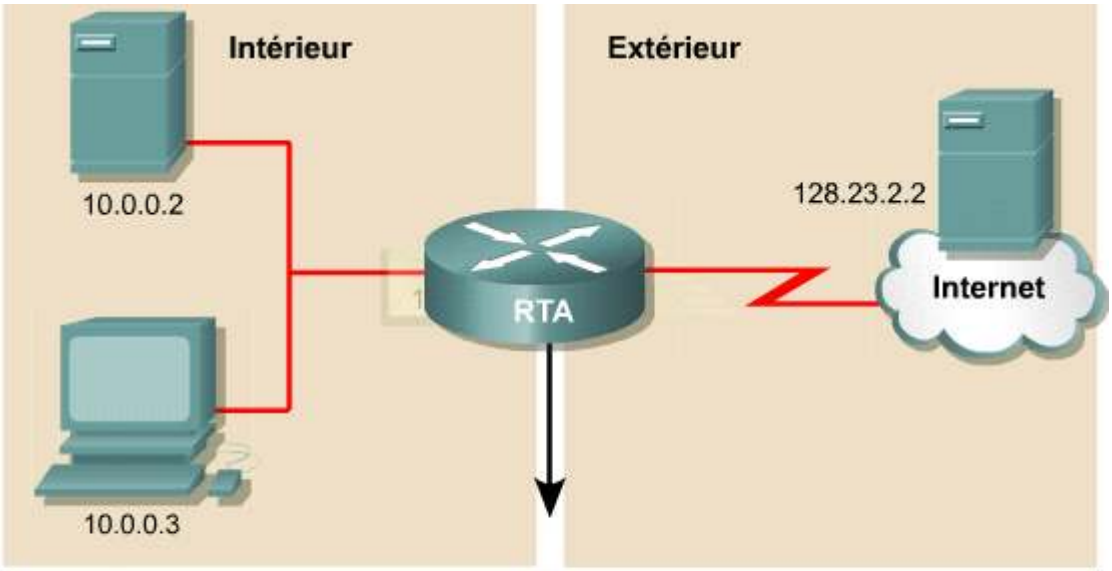


Table NAT		
Adresse IP locale interne	Adresse IP globale interne	Adresse IP globale externe
10.0.0.3	179.9.8.80	128.23.2.2

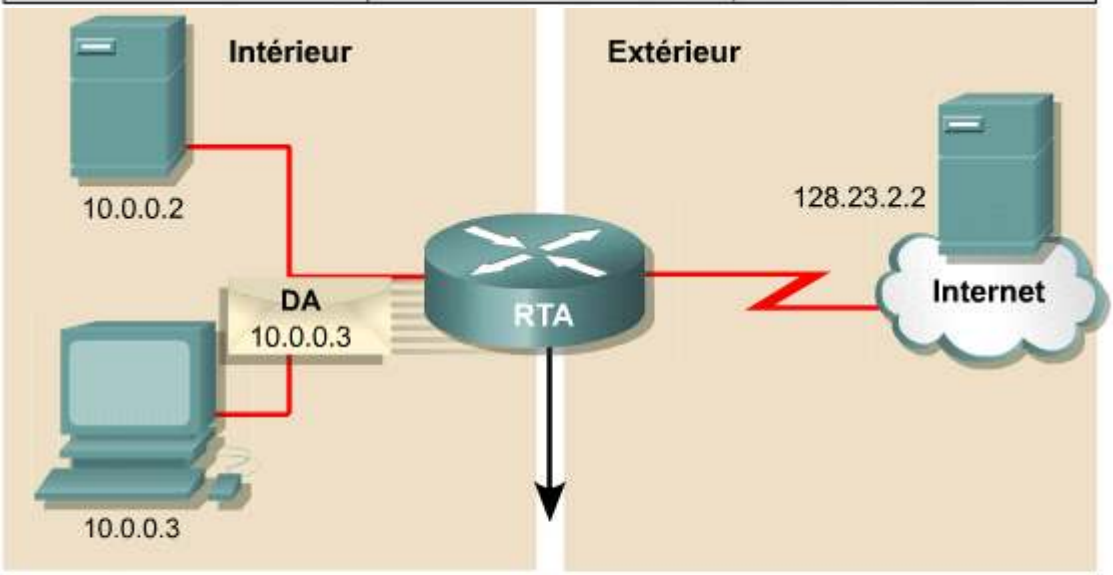


Table NAT		
Adresse IP locale interne	Adresse IP globale interne	Adresse IP globale externe
10.0.0.3	179.9.8.80	128.23.2.2

Dans la terminologie de NAT, le réseau interne désigne l'ensemble des réseaux soumis à la traduction. Toutes les autres adresses appartiennent au réseau externe.

Les termes ci-dessous, liés à NAT, ont été définis par Cisco:

- **Adresse locale interne** – L'adresse IP attribuée à un hôte du réseau interne. Il ne s'agit généralement pas d'une adresse IP assignée par l'organisme InterNIC (*Internet Network Information Center*) ou le fournisseur d'accès. Cette adresse est probablement une adresse privée RFC 1918.
- **Adresse globale interne** – Une adresse IP légitime attribuée par InterNIC ou par le fournisseur d'accès, et qui représente une ou plusieurs adresses IP locales internes pour le monde extérieur.
- **Adresse locale externe** – L'adresse IP d'un hôte externe telle que la connaissent les hôtes du réseau interne.
- **Adresse globale externe** – L'adresse IP attribuée à un hôte du réseau externe. C'est le propriétaire de l'hôte qui attribue cette adresse.

Activité de média interactive

Glisser-Positionner: Traduction d'adresses réseau de base

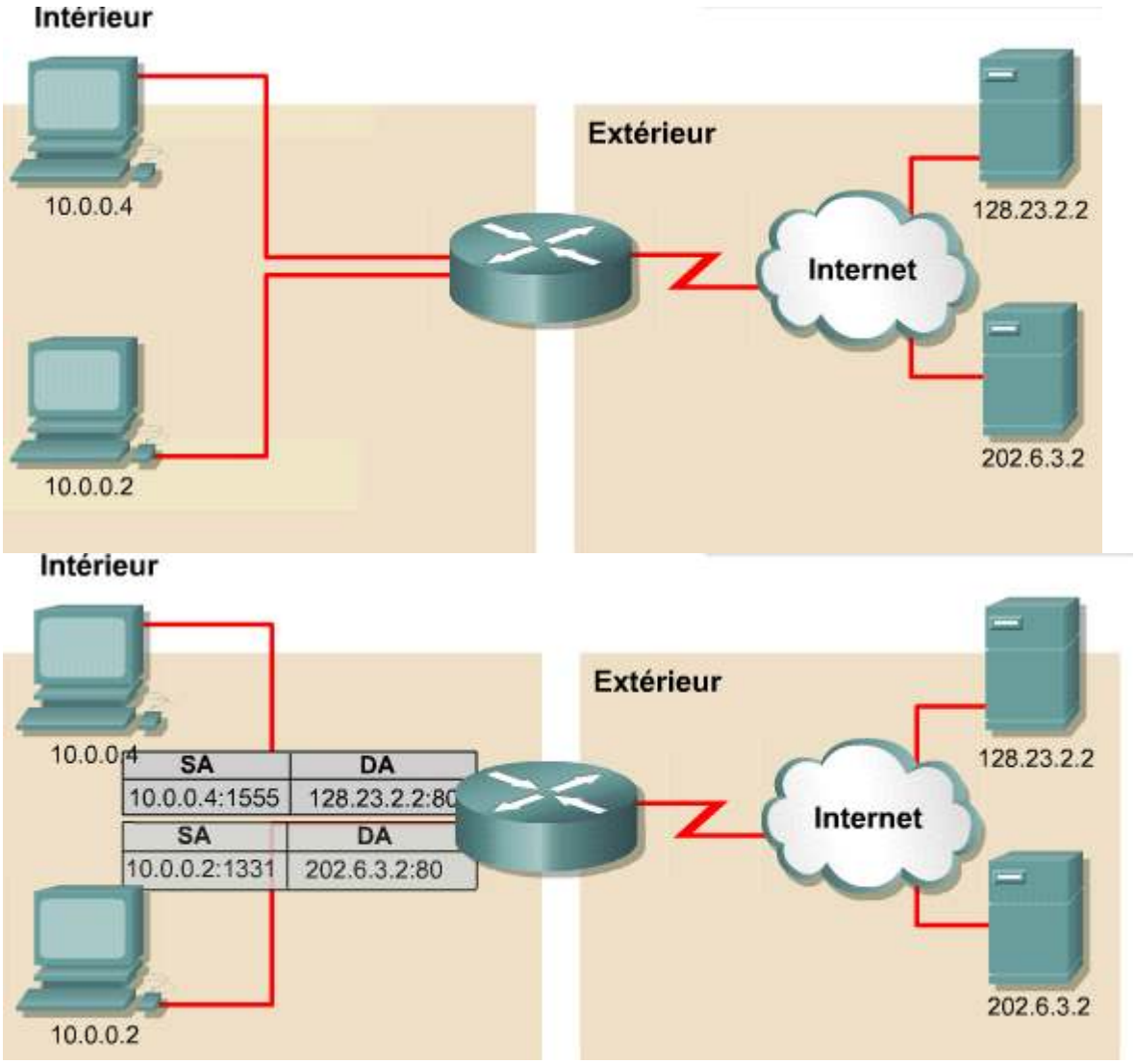
À la fin de cette activité, l'étudiant sera en mesure d'identifier les traductions d'adresses réseau qui s'effectuent lors de l'utilisation de la fonction NAT.

1.1 Évolutivité des réseaux avec NAT et PAT

1.1.3 Principales fonctionnalités NAT et PAT

Les traductions NAT peuvent avoir de nombreuses utilisations et peuvent indifféremment être attribuées de façon statique ou dynamique. La fonction NAT statique est conçue pour permettre le mappage bi-univoque d'adresses locales et globales. Ceci s'avère particulièrement utile pour les hôtes qui doivent disposer d'une adresse permanente, accessible depuis Internet. Ces hôtes internes peuvent être des serveurs d'entreprise ou des équipements de réseau.

La fonction NAT dynamique est conçue pour mapper une adresse IP privée sur une adresse publique. Une adresse IP quelconque prise dans un groupe d'adresses IP publiques est attribuée à un hôte du réseau. En cas de surcharge, ou avec la traduction d'adresses de ports (*Port Address Translation* - PAT), plusieurs adresses IP privées peuvent être mappées sur une adresse IP publique unique. Comme le suivi des adresses privées se fait sur le numéro de port, plusieurs adresses peuvent être mappées sur une adresse unique. [1]



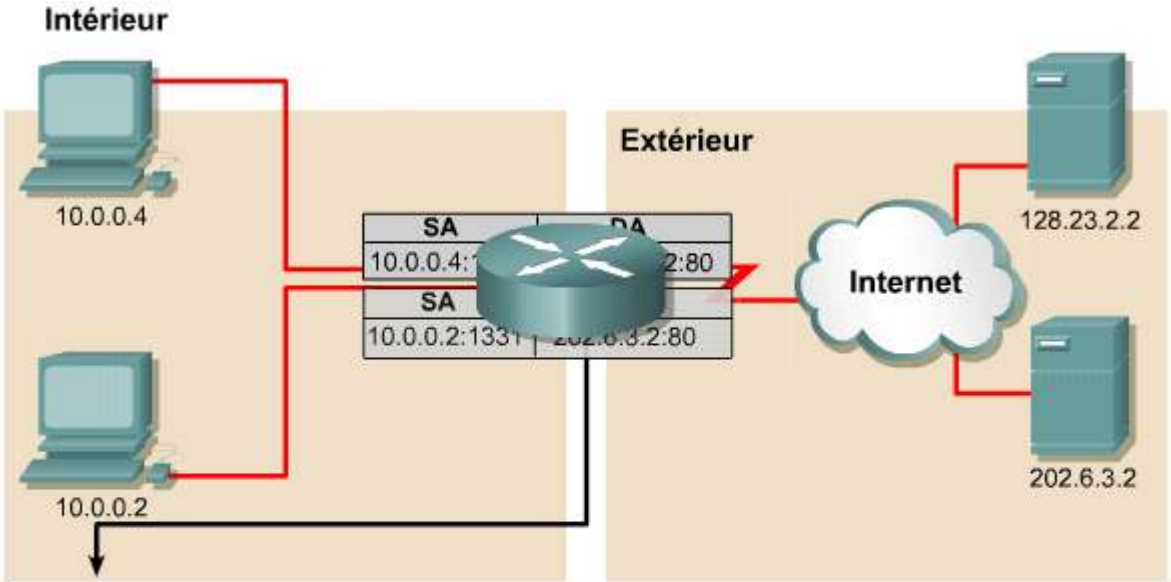


Table NAT avec surcharge			
Adresse IP locale interne	Adresse IP globale interne	Adresse IP locale externe	Adresse globale externe
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

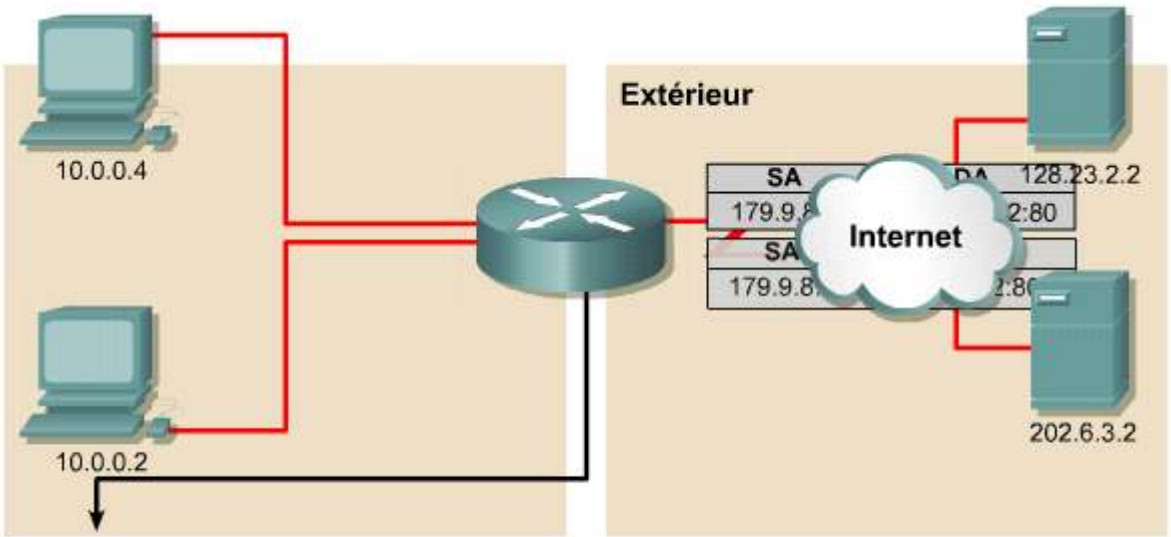


Table NAT avec surcharge			
Adresse IP locale interne	Adresse IP globale interne	Adresse IP locale externe	Adresse globale externe
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

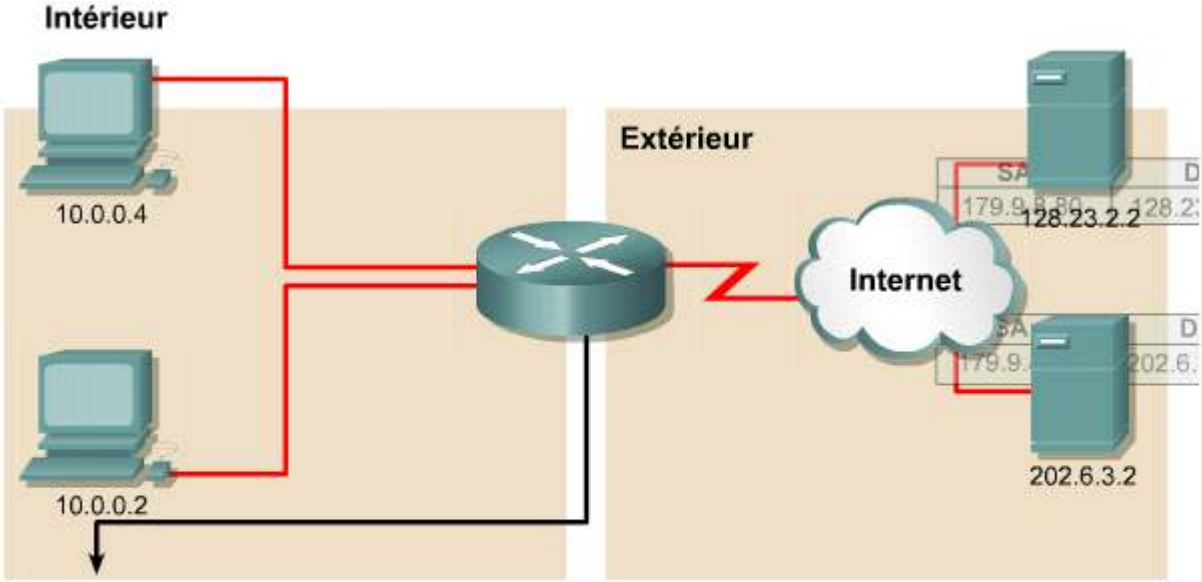
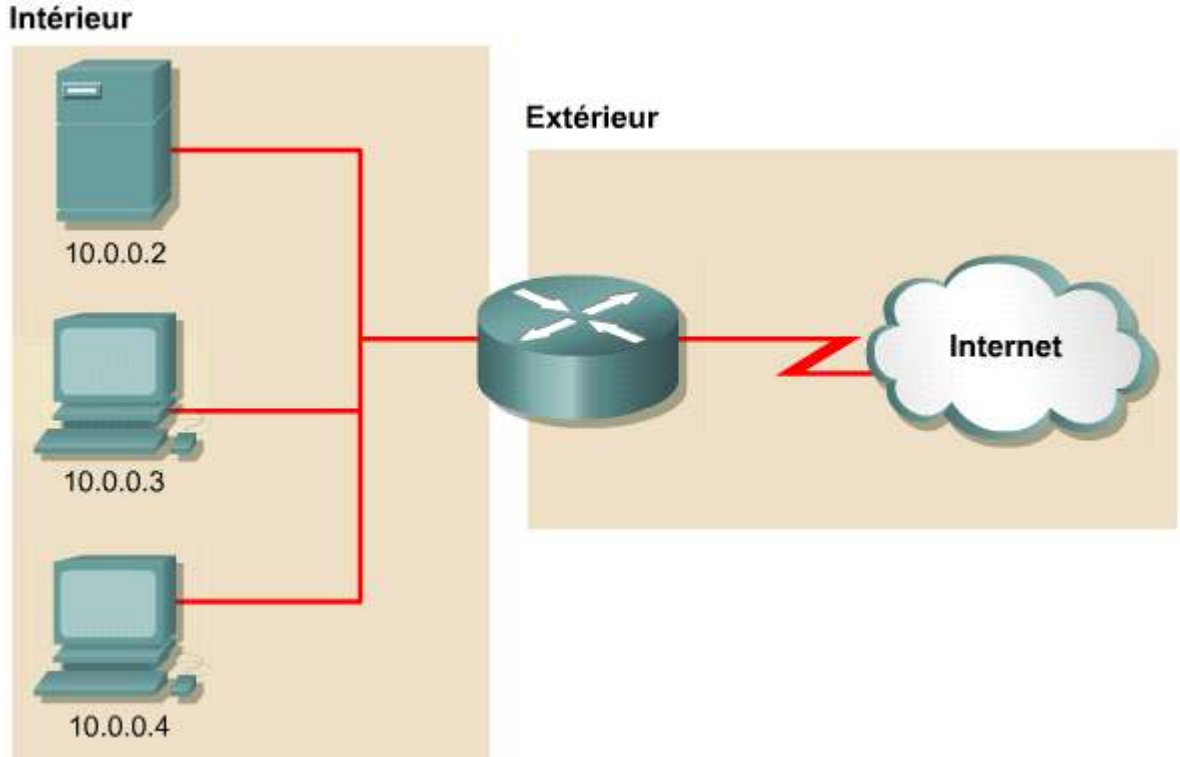
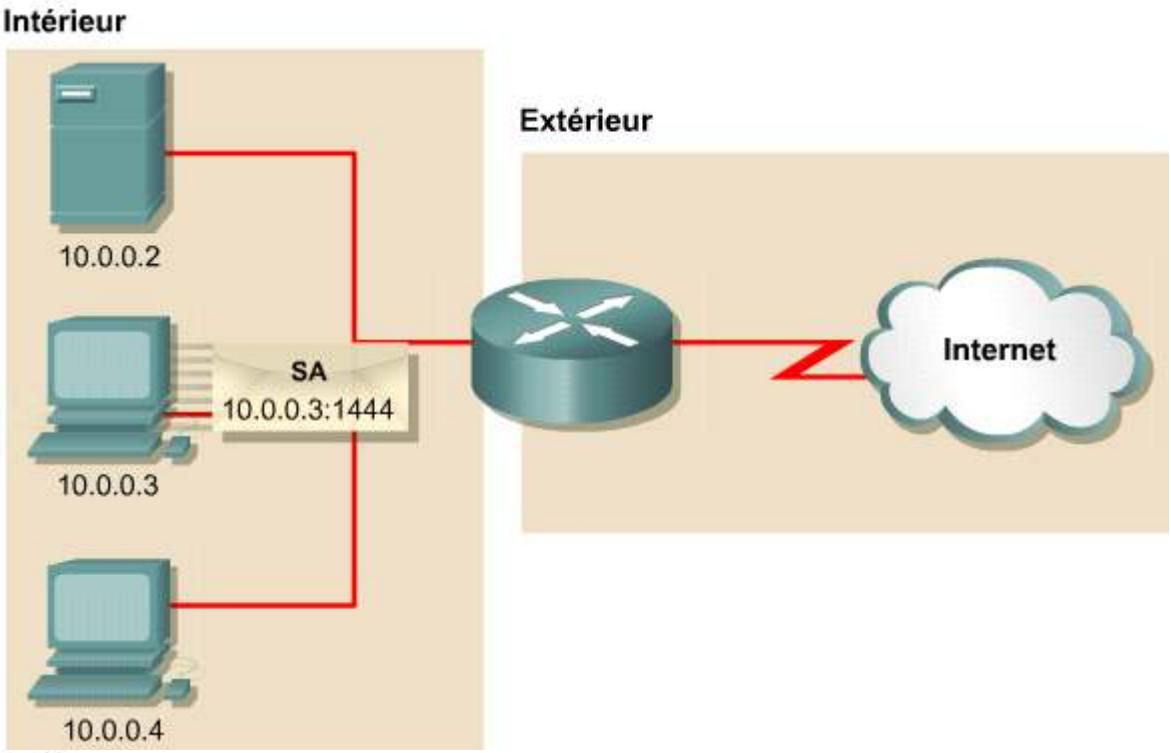


Table NAT avec surcharge			
Adresse IP locale interne	Adresse IP globale interne	Adresse IP locale externe	Adresse globale externe
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

La fonction PAT utilise des numéros de port source uniques sur l'adresse IP globale interne, de façon à assurer une distinction entre les traductions. 2





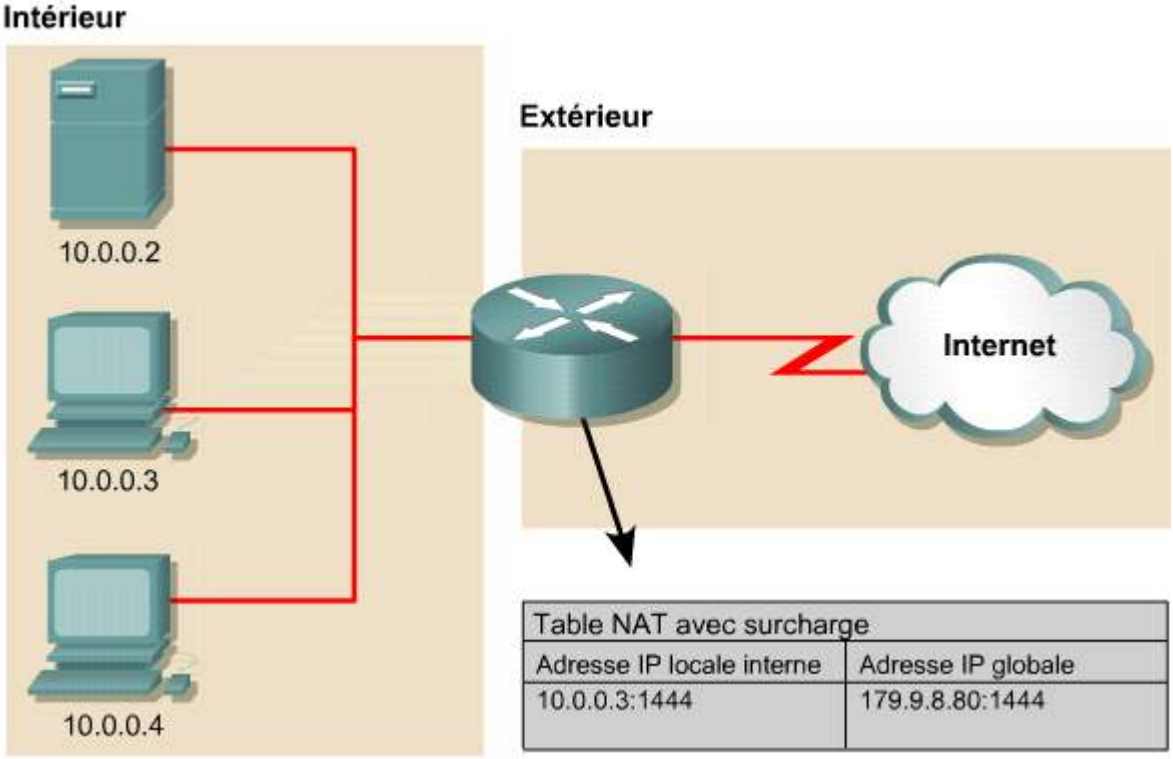


Table NAT avec surcharge	
Adresse IP locale interne	Adresse IP globale
10.0.0.3:1444	179.9.8.80:1444

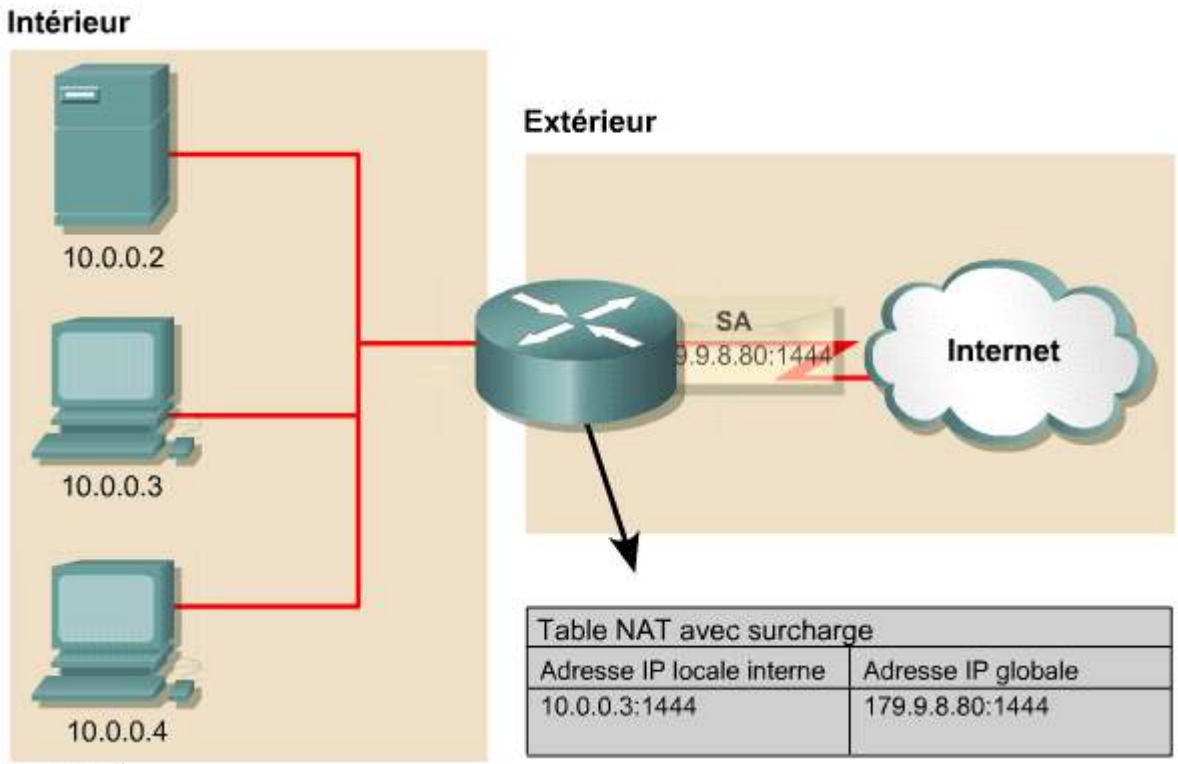
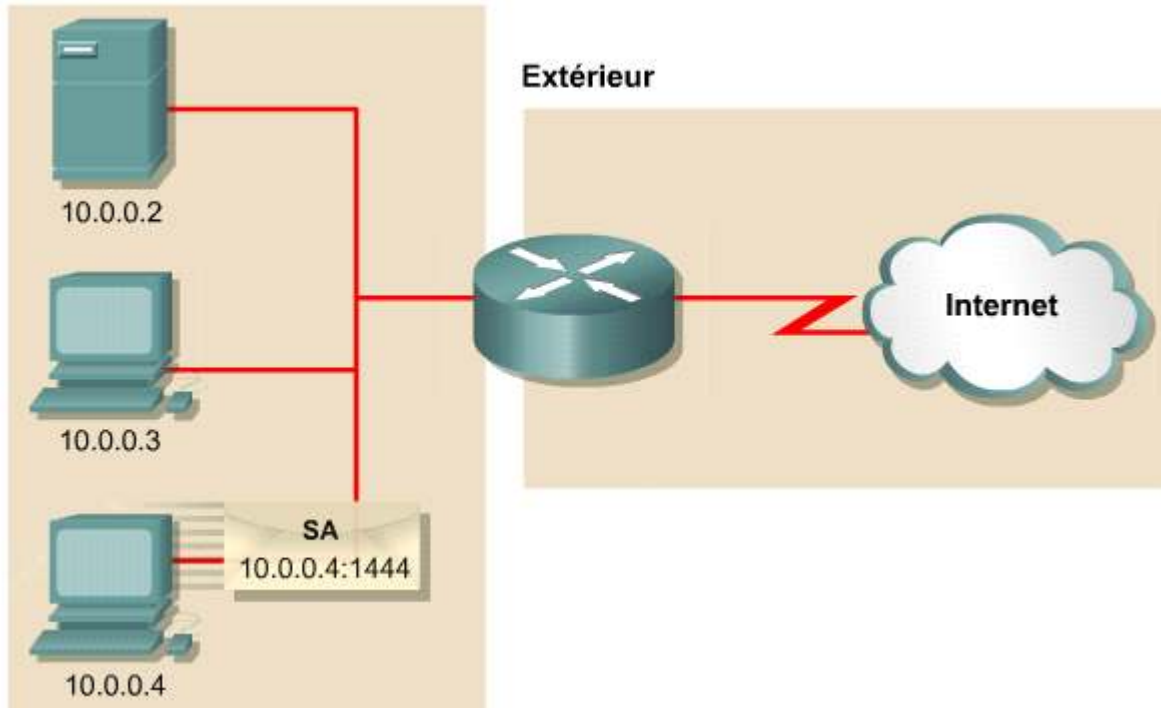
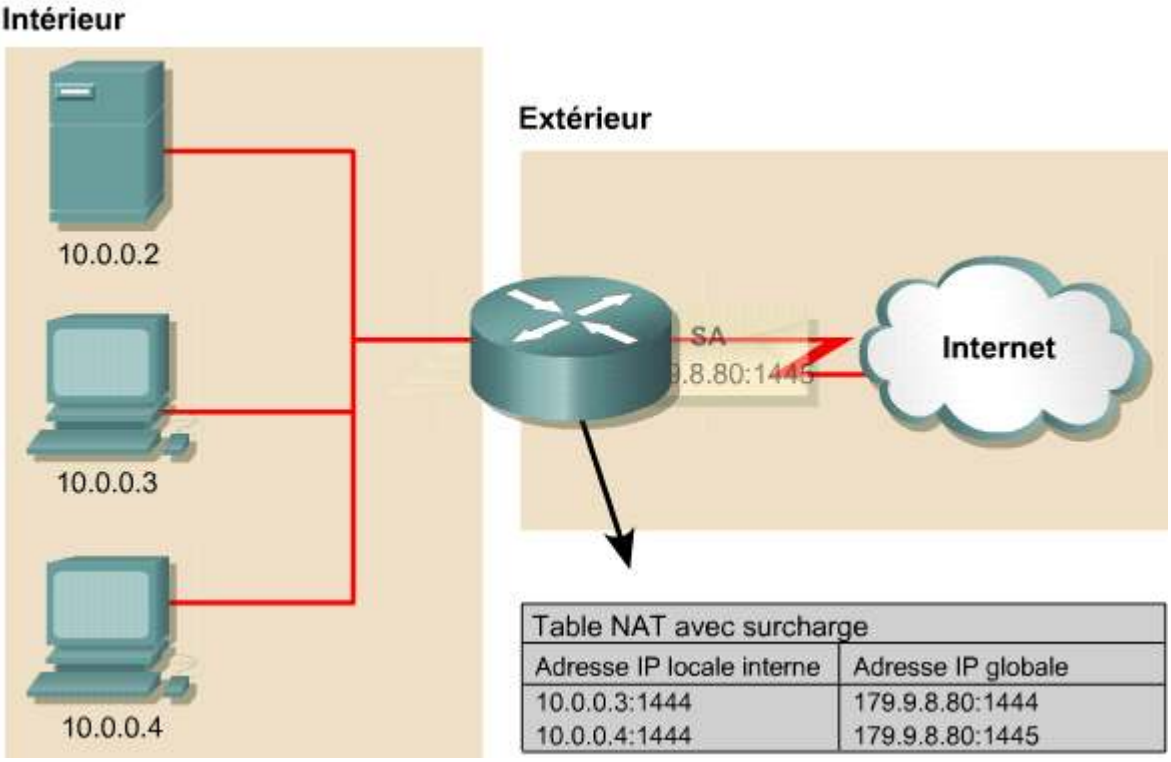


Table NAT avec surcharge	
Adresse IP locale interne	Adresse IP globale
10.0.0.3:1444	179.9.8.80:1444





Le numéro de port est encodé sur 16 bits. Le nombre total d'adresses internes pouvant être traduites en une adresse externe peut théoriquement atteindre les 65 536 par adresse IP. De façon plus réaliste, le nombre de port pouvant être attribués à une adresse IP unique avoisine les 4000. La fonction PAT tente de conserver le port source d'origine. Si ce port source est déjà utilisé, PAT attribue le premier numéro de port disponible en commençant au début du groupe de ports approprié, à savoir 0-511, 512-1023, ou 1024-65535. Quand il n'y a plus de ports disponibles et que plusieurs adresses IP externes sont configurées, PAT sélectionne l'adresse IP suivante pour tenter d'allouer de nouveau le numéro du port source initial. Ce processus se poursuit jusqu'à ce qu'il ait épuisé les ports et les adresses IP externes disponibles.

La fonction NAT offre les avantages suivants:

- Elle élimine le besoin de réattribuer une nouvelle adresse IP à chaque hôte lors du passage à un nouveau FAI. NAT élimine le besoin de réadresser tous les hôtes qui nécessitent un accès externe, économisant ainsi du temps et de l'argent.
- Elle économise les adresses au moyen d'un multiplexage au niveau du port de l'application. Avec PAT, plusieurs hôtes internes peuvent partager une même adresse IP pour toutes leurs communications externes. Dans ce type de configuration, il suffit d'un très petit nombre d'adresses externes pour desservir un grand nombre d'hôtes internes, d'où une importante économie d'adresses IP.
- Elle protège le réseau. En effet, comme les réseaux privés ne divulguent pas leurs adresses ou leur topologie interne, ils restent raisonnablement sécurisés quand ils sont utilisés conjointement à la fonction NAT pour obtenir un accès externe.

Activité de média interactive

Glisser-Positionner: Traduction d'adresses réseau (NAT) avec surcharge

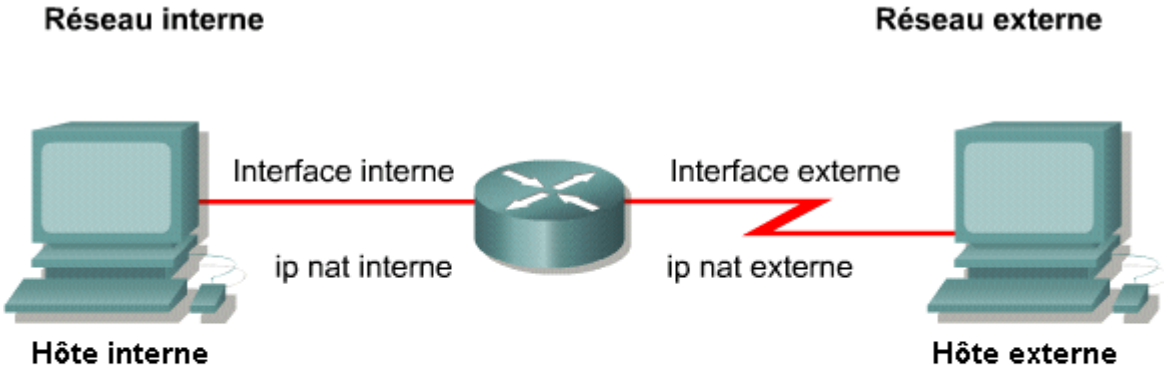
À la fin de cette activité, l'étudiant sera en mesure d'identifier les traductions d'adresses et de ports réseau qui s'effectuent lors de l'utilisation de la fonction PAT.

Traduction statique
Pour configurer une traduction statique d'adresses sources internes, effectuez les activités des figures 1 et 2.

```
Router(config)#ip nat inside source static 10.6.1.20 171.69.68.10
```

- Les traductions statiques sont entrées directement dans la configuration et résident toujours dans la table de traduction

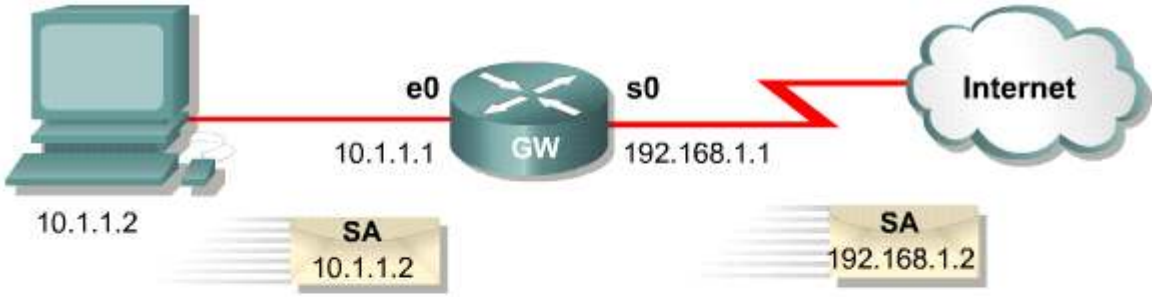
Étape	Action	Remarques :
1	Établissez la traduction statique entre une adresse locale interne et une adresse globale interne. `Router(config)#ip nat inside source static local-ip global-ip`	Entrez la commande globale **`no ip nat inside source static`** pour supprimer la traduction
2	Spécifiez l'interface interne. `Router(config)#interface numéro type`	Entrez la commande **`interface`**. L'invite CLI passe de `(config)#` à `(config-if)#`.
3	Signalez l'interface comme connectée à l'intérieur. `Router(config-if)#ip nat inside`	
4	Quittez le mode de configuration d'interface. `Router(config-if)#exit`	
5	Spécifiez l'interface externe. `Router(config)#interface numéro type`	
6	Signalez l'interface comme connectée à l'extérieur. `Router(config-if)#ip nat outside`	




```
Router(config-if)#ip nat interne
```

- Une interface sur le routeur peut être définie comme interne ou externe.
- Les traductions se produisent entre les interfaces internes et externes.

La figure 3 présente l'utilisation de la traduction NAT statique. Le routeur traduit les paquets de l'hôte 10.1.1.2 en l'adresse source 192.168.1.2.




```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Traduction dynamique

Pour configurer une traduction dynamique d'adresses sources internes, effectuez les activités de la figure 4

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
```

- Les listes d'accès sont utilisées par la fonction NAT pour sélectionner les adresses en vue d'une traduction dynamique

```
Router(config)#ip nat inside source list 1 pool nat-pool
```

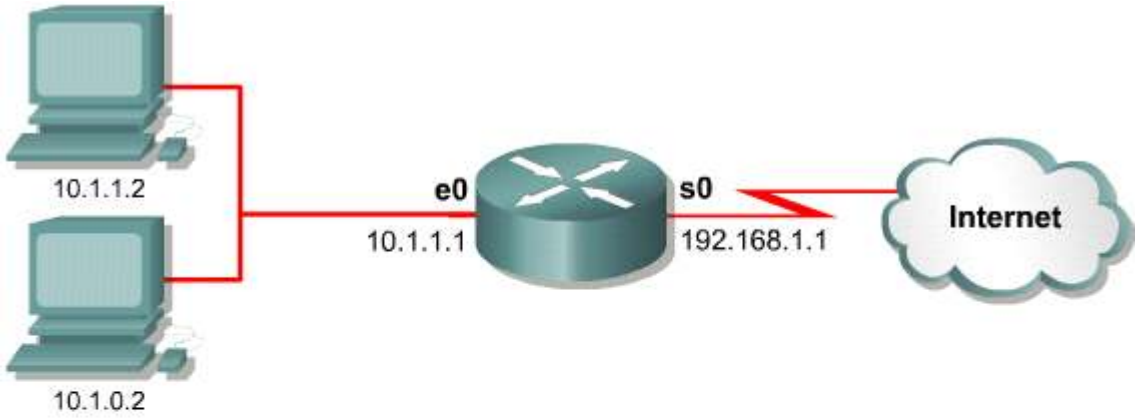
- La traduction dynamique utilise les adresses que la liste d'accès permet de traduire.

Étape	Action	Remarques
1	Définissez un groupe d'adresses globales à allouer selon les besoins. `Router(config)#ip nat pool name` *ip début ip fin* {`netmask` *masque réseau*|`prefix-length` *longueur préfixe*}	Entrez la commande globale `no ip nat pool` *nom* pour supprimer le groupe d'adresses globales.
2	Définissez une liste d'accès standard autorisant les adresses qui doivent être traduites. `Router(config)#access-list` numéro liste d'accès `permit` source [masque générique source]	Entrez la commande globale `no access-list` *numéro liste d'accès* pour supprimer la liste d'accès.
3	Établissez une traduction dynamique de la source, en spécifiant la liste d'accès définie à l'étape précédente. `Router(config)#ip nat inside source list` *numéro liste d'accès* `pool` *nom*	Entrez la commande globale `no ip nat inside source` pour supprimer la traduction dynamique source.
4	Spécifiez l'interface interne. `Router(config)#interface` *numéro type*	Entrez la commande `interface`. L'invite CLI passe de `(config)#` à `(config-if)#`.
5	Signalez l'interface comme connectée à l'intérieur. `Router(config-if)#ip nat inside`	
6	Quittez le mode de configuration d'interface. `Router(config-if)#exit`	
7	Spécifiez l'interface externe. `Router(config)#interface` *numéro type*	
8	Signalez l'interface comme connectée à l'extérieur. `Router(config-if)#ip nat outside`	

.

La liste d'accès doit seulement autoriser les adresses à traduire. N'oubliez pas que chaque liste de contrôle d'accès est exclusive («deny all» implicite à la fin). Une liste d'accès trop laxiste peut mener à des résultats imprévisibles. Cisco recommande de ne pas configurer les listes d'accès référencées par des commandes NAT à l'aide de la commande **`permit any`**. En effet, **`permit any`** peut mener la fonction NAT à consommer trop de ressources routeur, ce qui peut occasionner des problèmes sur le réseau.

La figure 5 traduit toutes les adresses sources à partir de 10.1.0.0/24 acceptées par la liste d'accès 1 en une adresse du groupe dénommé nat-pool1. Le groupe contient les adresses de 179.9.8.80/24 à 179.9.8.95/24.




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

REMARQUE:
NAT ne traduit pas l'hôte 10.1.1.2, car cette traduction n'est pas autorisée par la liste d'accès.

Surcharge
Il existe deux façons de configurer la surcharge, en fonction de la manière dont les adresses IP publiques ont été allouées. Un FAI ne peut allouer qu'une adresse IP publique à un réseau, en l'assignant généralement à l'interface externe qui assure la connexion. La figure 6 montre comment configurer la surcharge dans cette situation.

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
```

• Définit une liste d'accès IP standard autorisant les adresses locales internes qui doivent être traduites.

```
Router(config)#ip nat inside source list 1 interface serial0/0
overload
```

• Établit la traduction de surcharge, en spécifiant les adresses IP à surcharger comme attribuées à une interface externe

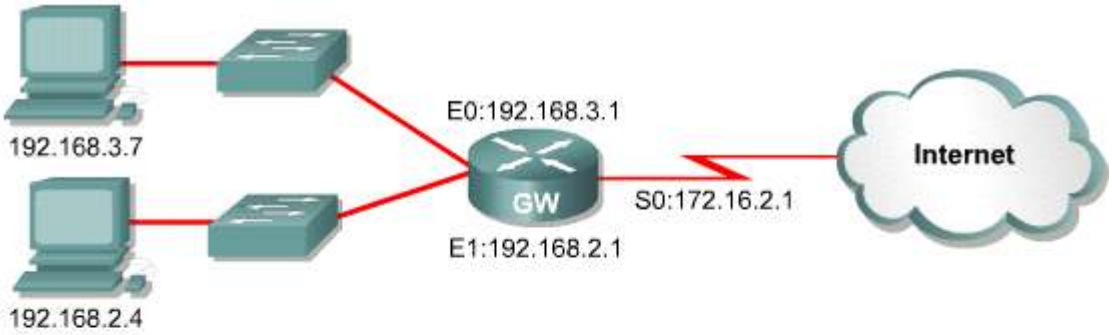
Step	Action	Remarques
1	Définissez une liste d'accès standard autorisant les adresses qui doivent être traduites. `Router(config)#access-list` *numéro acl source [masque générique source]*	Entrez la commande globale `no access-list` *numéro liste d'accès* pour supprimer la liste d'accès.
2A	Établissez une traduction dynamique de la source, en spécifiant la liste d'accès définie à l'étape précédente. `Router(config)#ip nat inside source list` *numéro acl* `interface` *interface* `overload`	Entrez la commande globale `no ip nat inside source` pour supprimer la traduction dynamique source. Le mot clé `overload` active la fonction PAT.
2B	Spécifiez l'adresse globale, en tant que groupe, à utiliser pour la surcharge. `Router(config)#ip nat pool` *nom ip début ip fin* {`netmask` *masque de réseau* | `prefix-length` *longueur préfixe*} Établissez la traduction de surcharge. `Router {config}#ip nat inside source list` *numéro acl* `pool` *nom* `overload`	
3	Spécifiez l'interface interne. `Router(config)#interface` *numéro type* `Router(config-if)#ip nat inside`	Entrez la commande `interface`. L'invite CLI passe de `(config)#` à `(config-if)#`.
4	Spécifiez l'interface externe. `Router(config-if)#interface` *numéro type* `Router(config-if)#ip nat outside`	

L'autre méthode de configuration de la surcharge est valable si le FAI a fourni une ou plusieurs adresses IP publiques à titre de groupe NAT. Ce groupe peut être surchargé comme dans la configuration illustrée à la figure 7.

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255

Router(config)#ip nat pool nat-pool2 179.9.8.20 netmask
255.255.255.240

Router(config)#ip nat inside source list 1 pool nat-pool2
overload
```

• Établit la traduction de surcharge et spécifie l'adresse IP à surcharger comme celle désignée dans le groupe.

La figure 8 montre un exemple de configuration PAT.




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Activité de TP

Exercice: Configuration de la fonction NAT

Au cours de ce TP, un routeur va être configuré en vue d'utiliser la traduction d'adresses réseau (NAT).

Activité de TP

Exercice: Configuration de la fonction PAT

Au cours de ce TP, un routeur va être configuré en vue d'utiliser la traduction d'adresses de ports (PAT).

Activité de TP

Exercice: Configuration d'adresses NAT statiques

Au cours de ce TP, un routeur va être configuré en vue d'utiliser la traduction d'adresses réseau (NAT) pour convertir des adresses IP internes, généralement privées, en des adresses publiques externes.

Activité de TP

Activité en ligne: Configuration de la fonction NAT

Au cours de ce TP, l'étudiant va configurer la fonction NAT.

Activité de TP

Activité en ligne: Configuration de la fonction PAT

Au cours de ce TP, les étudiants vont configurer un routeur en vue d'utiliser la traduction d'adresses de ports (PAT) pour convertir des adresses IP internes, généralement privées, en des adresses publiques externes.

Activité de TP

Activité en ligne: Configuration d'adresses NAT statiques

Au cours de ce TP, l'étudiant va configurer un routeur en vue d'utiliser la traduction d'adresses réseau (NAT) pour convertir des adresses IP internes, généralement privées, en des adresses publiques externes.

1.1 Évolutivité des réseaux avec NAT et PAT

1.1.5 Vérification de la configuration PAT

Une fois la fonction NAT configurée, utilisez les commandes **clear** et **show** pour vous assurer qu'elle fonctionne correctement.

Par défaut, les traductions d'adresse dynamiques deviennent inactives dans la table de traduction NAT au terme d'une période de non-utilisation. Si la traduction de port n'est pas configurée, les entrées de traduction se désactivent au bout de 24 heures, sauf si les temporisations ont été reconfigurées par la commande **ip nat translation timeout** *timeout_seconds* du mode de configuration globale. Annulez les entrées avant l'écoulement du délai à l'aide de l'une des commandes présentées à la figure 1.

```
Router#clear ip nat translation *
```

• Efface toutes les entrées de traduction dynamique d'adresses

```
Router#clear ip nat translation inside global-ip local-ip [outside
local-ip global-ip]
```

• Efface une entrée simple de traduction dynamique

```
Router#clear ip nat translation protocol inside global-ip global-port
local-ip local-port [outside local-ip local-port global-ip
global-port]
```

• Efface une entrée étendue de traduction dynamique

Commande	Description
clear ip nat translation *	Efface toutes les entrées de traduction dynamique d'adresses de la table de traduction NAT
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Efface une entrée de traduction dynamique simple contenant une traduction interne ou une traduction à la fois interne et externe
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Efface une entrée étendue de traduction dynamique

Vous pouvez afficher les informations de traduction en effectuant l'une des activités en mode EXEC 2.

```
Router#show ip nat translations [verbose]
```

* verbose (facultatif) Affiche des informations complémentaires pour chaque entrée de la table de traduction, notamment le temps écoulé depuis la création et l'utilisation de l'entrée

```
Router#show ip nat translations
Pro Inside global     Inside local      Outside local  Outside global
172.16.131.1          10.10.10.1             ---            ---
```

```
Router#show ip nat statistics
```

• Affiche les statistiques de traduction

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Commande	Description
show ip nat translations	Affiche les traductions actives
show ip nat statistics	Affiche les statistiques de traduction

Vous pouvez également utiliser la commande **show run** et rechercher les commandes NAT, de liste d'accès, d'interface ou de groupe qui présentent les valeurs requises.

Activité de TP

Exercice: Vérification de la configuration des fonctions NAT et PAT

Au cours de ce TP, les étudiants vont configurer un routeur pour la traduction d'adresses réseau (NAT) et la traduction d'adresses de ports (PAT).

Activité de TP

Activité en ligne: Vérification de la configuration des fonctions NAT et PAT

Au cours de ce TP, les étudiants vont configurer un routeur pour la traduction d'adresses réseau (NAT) et la traduction d'adresses de ports (PAT).

1.1 Évolutivité des réseaux avec NAT et PAT

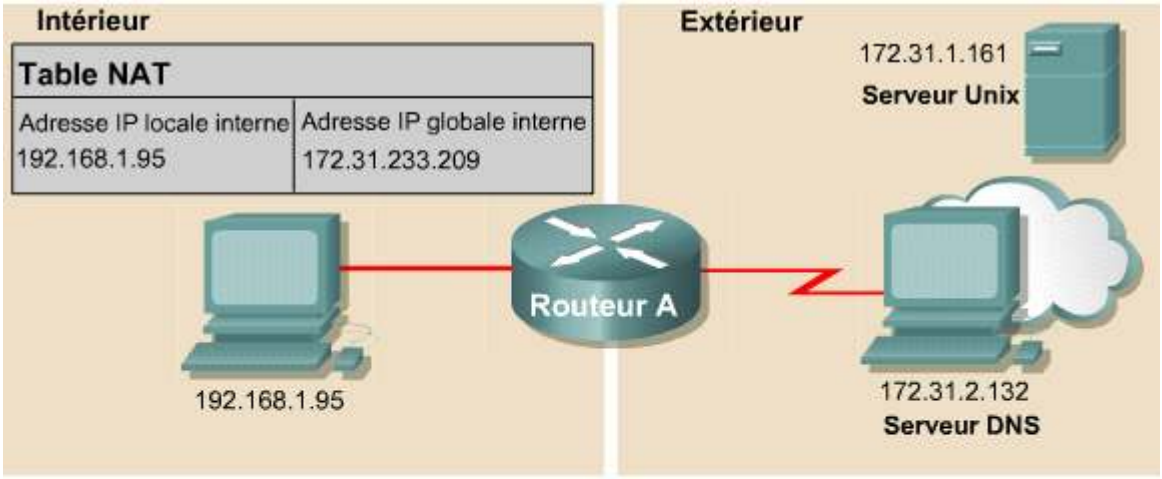
1.1.6 Dépannage de la configuration des fonctions NAT et PAT

Quand des problèmes de connectivité IP surviennent dans un environnement NAT, il s'avère parfois difficile d'en déterminer la cause. Il arrive souvent que la fonction NAT soit mise en cause, alors qu'il s'agit en réalité d'un problème sous-jacent.

Lorsque vous essayez de déterminer la cause d'un problème de connectivité IP, il peut s'avérer utile de mettre la fonction NAT hors de cause. Procédez comme suit pour déterminer si NAT fonctionne correctement:

1. À partir de la configuration, définissez clairement ce que la fonction NAT est censée faire.
2. Assurez-vous que les traductions appropriées sont présentes dans la table de traduction.
3. Assurez-vous que la traduction s'effectue en exécutant les commandes **show** et **debug**.
4. Vérifiez de façon détaillée ce qui arrive au paquet et assurez-vous que les routeurs disposent des informations correctes pour l'acheminer.

Utilisez la commande **debug ip nat** pour vérifier le fonctionnement de la fonction NAT en affichant des informations sur chacun des paquets traduits par le routeur. La commande **debug ip nat detailed** génère une description individuelle des paquets dont la traduction est envisagée. Cette commande renvoie également des informations sur certaines erreurs ou conditions d'exception, par exemple l'impossibilité d'allouer une adresse globale.




```
RouteurA#debug ip nat
NAT:   s= 192.168.1.95   ---> 172.31.233.209,        d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,     d=172.31.233.209,    ---> 192.168.1.95 [21852]
NAT:   s= 192.168.1.95   ---> 172.31.233.209,        d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,    ---> 192.168.1.95 [23311]
NAT*:  s= 192.168.1.95   ---> 172.31.233.209,        d=172.31.1.161 [6827]
NAT*:  s= 192.168.1.95   ---> 172.31.233.209,        d=172.31.1.161 [6828]
NAT*:  s= 172.31.1.161      d=172.31.233.209,    ---> 192.168.1.95 [23313]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,    ---> 192.168.1.95 [23313]
```

La figure 1 montre un exemple de résultats de **debug ip nat**. Dans cet exemple, les deux premières lignes des résultats de débogage montrent qu'une requête et une réponse DNS ont été produites. Les lignes restantes montrent les résultats de débogage d'une connexion Telnet d'un hôte interne au réseau vers un hôte externe.

Décodez les résultats de **debug** à l'aide des points clés suivants :

- L'astérisque en regard de NAT indique que la traduction s'effectue sur le chemin à commutation rapide. Le premier paquet d'une conversation emprunte toujours la voie lente, ce qui indique qu'il est commuté par le processus. Les paquets restants passent par le chemin à commutation rapide s'il existe une entrée en mémoire cache.
- s = a.b.c.dest l'adresse source.
- L'adresse source a.b.c.d est traduite en w.x.y.z.
- d = e.f.g.h est l'adresse de destination.
- La valeur entre parenthèses représente le numéro d'identification IP. Ces informations peuvent s'avérer utiles pour le débogage. Par exemple, elles permettent d'établir une corrélation avec d'autres traces de paquets provenant d'analyseurs de protocole.

Activité de TP

Exercice: Dépannage des fonctions NAT et PAT

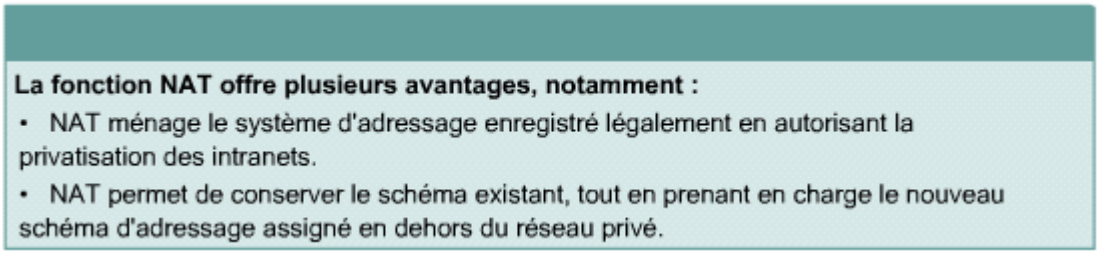
Au cours de ce TP, les étudiants vont configurer et dépanner un routeur pour la traduction d'adresses réseau (NAT) et la traduction d'adresses de ports (PAT).

Activité de TP

Activité en ligne: Dépannage des fonctions NAT et PAT

Au cours de ce TP, les étudiants vont configurer et dépanner un routeur pour la traduction d'adresses réseau (NAT) et la traduction d'adresses de ports (PAT).

La fonction NAT offre plusieurs avantages, notamment: 1


La fonction NAT offre plusieurs avantages, notamment :
• NAT ménage le système d'adressage enregistré légalement en autorisant la privatisation des intranets.
• NAT permet de conserver le schéma existant, tout en prenant en charge le nouveau schéma d'adressage assigné en dehors du réseau privé.

- Elle ménage le système d'adressage enregistré légalement en autorisant la privatisation des intranets.
- Elle augmente la souplesse des connexions vers le réseau public. Il est possible de définir des groupes multiples, des groupes de sauvegarde et des groupes d'équilibrage de charge pour assurer des connexions plus fiables au réseau public.
- Cohérence du système d'adressage du réseau interne. Sur un réseau sans adresses IP privées et sans traduction NAT, le changement des adresses IP publiques oblige à renuméroter tous les hôtes du réseau. La renumérotation des hôtes peut représenter des coûts non négligeables. La fonction NAT permet de conserver le système existant, tout en prenant en charge un nouveau système d'adressage public.

Toutefois, NAT présente certains inconvénients. L'activation de la traduction d'adresse entraîne une perte de fonctionnalité, en particulier avec les protocoles ou les applications qui impliquent l'envoi d'adresses IP à l'intérieur des données utiles du paquet IP. Ceci nécessite un traitement supplémentaire par l'équipement effectuant la traduction NAT.

NAT augmente les délais. Des délais de commutation de chemin sont introduits par la traduction de chaque adresse IP à l'intérieur des en-têtes de paquet. Le premier paquet emprunte toujours le chemin lent, ce qui signifie qu'il subit une commutation de processus. Les paquets restants passent par le chemin à commutation rapide s'il existe une entrée en mémoire cache.

Les performances peuvent constituer un problème, car à l'heure actuelle, la fonction NAT est accomplie au moyen d'une commutation de processus. Le processeur examine chaque paquet pour déterminer s'il doit être ou non traduit. Il doit modifier l'en-tête IP, et éventuellement l'en-tête TCP.

L'un des inconvénients significatifs de la mise en oeuvre et de l'utilisation de NAT est la perte de traçabilité IP de bout en bout. Il devient bien plus difficile de suivre les paquets qui subissent de nombreux changements d'adresse sur plusieurs sauts NAT. Pour les pirates qui cherchent à déterminer la source d'un paquet, il est difficile de retracer ou d'obtenir les adresses source ou de destination initiales.

NAT force également certaines applications utilisant l'adressage IP à arrêter de fonctionner car elles masquent les adresses IP de bout en bout. Les applications qui utilisent des adresses physiques au lieu d'un nom de domaine qualifié n'atteignent pas les destinations qui sont traduites sur le routeur NAT. On peut parfois éviter ce problème par des mappages NAT statiques.

Cisco IOS NAT prend en charge les types de trafic ci-dessous: 2

Cisco IOS NAT prend en charge les types de trafic ci-dessous, bien qu'ils transportent les adresses IP dans le flux de données de l'application :
- ICMP
- Le protocole FTP (File Transfer Protocol), et notamment les commandes PORT et PASV
- Les services NetBIOS sur TCP/IP, de datagramme, de nom et de session
- Real Audio de Progressive Networks
- CUSeeMe de White Pines
- Les requêtes DNS " A " et " PTR "
- H.323/NetMeeting, versions 12.0(1)/12.0(1)T et ultérieures
- VDOLive, versions 11.3(4)/11.3(4)T et ultérieures
- Vxtreme, versions 11.3(4)/11.3(4)T et ultérieures
- IP Multicast, version 12.0(1)T, traduction d'adresses sources seulement

Cisco IOS NAT ne prend pas en charge les types de trafic ci-dessous :
- Les mises à jour de la table de routage
- Les transferts de zone DNS
- Le protocole BOOTP
- talk, ntalk
- Le protocole SNMP (Simple Network Management Protocol)

- Le protocole ICMP
- Le protocole FTP (*File Transfer Protocol*), et notamment les commandes PORT et PASV
- Les services NetBIOS sur TCP/IP, de datagramme, de nom et de session
- RealAudio de RealNetworks
- CUSeeMe de White Pines
- StreamWorks de Xing Technologies
- Requêtes DNS «A» et «PTR»
- H.323/Microsoft NetMeeting, IOS versions 12.0(1)/12.0(1)T et ultérieures
- VDOLive de VDOnet, IOS versions 11.3(4)/11.3(4)T et ultérieures
- Web Theater de VXtreme, IOS versions 11.3(4)11.3(4)T et ultérieures
- IP Multicast, IOS version 12.0(1)T avec traduction d'adresses sources seulement

Cisco IOS NAT ne prend pas en charge les types de trafic ci-dessous:

- Les mises à jour de la table de routage
- Les transferts de zone DNS
- Le protocole BOOTP
- Les protocoles talk et ntalk
- Le protocole SNMP (*Simple Network Management Protocol*)

Activité de média interactive

Case à cocher: Problèmes liés à la fonction NAT

Quand l'étudiant aura effectué cette activité, il sera en mesure d'identifier les problèmes relatifs à l'utilisation de la fonction NAT.

1.2.1 Présentation du protocole DHCP

Le protocole DHCP (*Dynamic Host Configuration Protocol*) fonctionne en mode client/serveur. Le protocole DHCP permet aux clients DHCP d'un réseau IP d'obtenir leurs configurations à partir d'un serveur DHCP. Avec le protocole DHCP, la gestion d'un réseau IP demande moins de travail. L'adresse IP est l'option de configuration la plus importante que le client reçoit du serveur. Le protocole DHCP est décrit dans la RFC 2131.

Un client DHCP est fourni avec la plupart des systèmes d'exploitation récents, notamment les divers systèmes Windows, Novell Netware, Sun Solaris, Linux et MAC OS. Le client demande des valeurs d'adressage au serveur DHCP du réseau. [1]

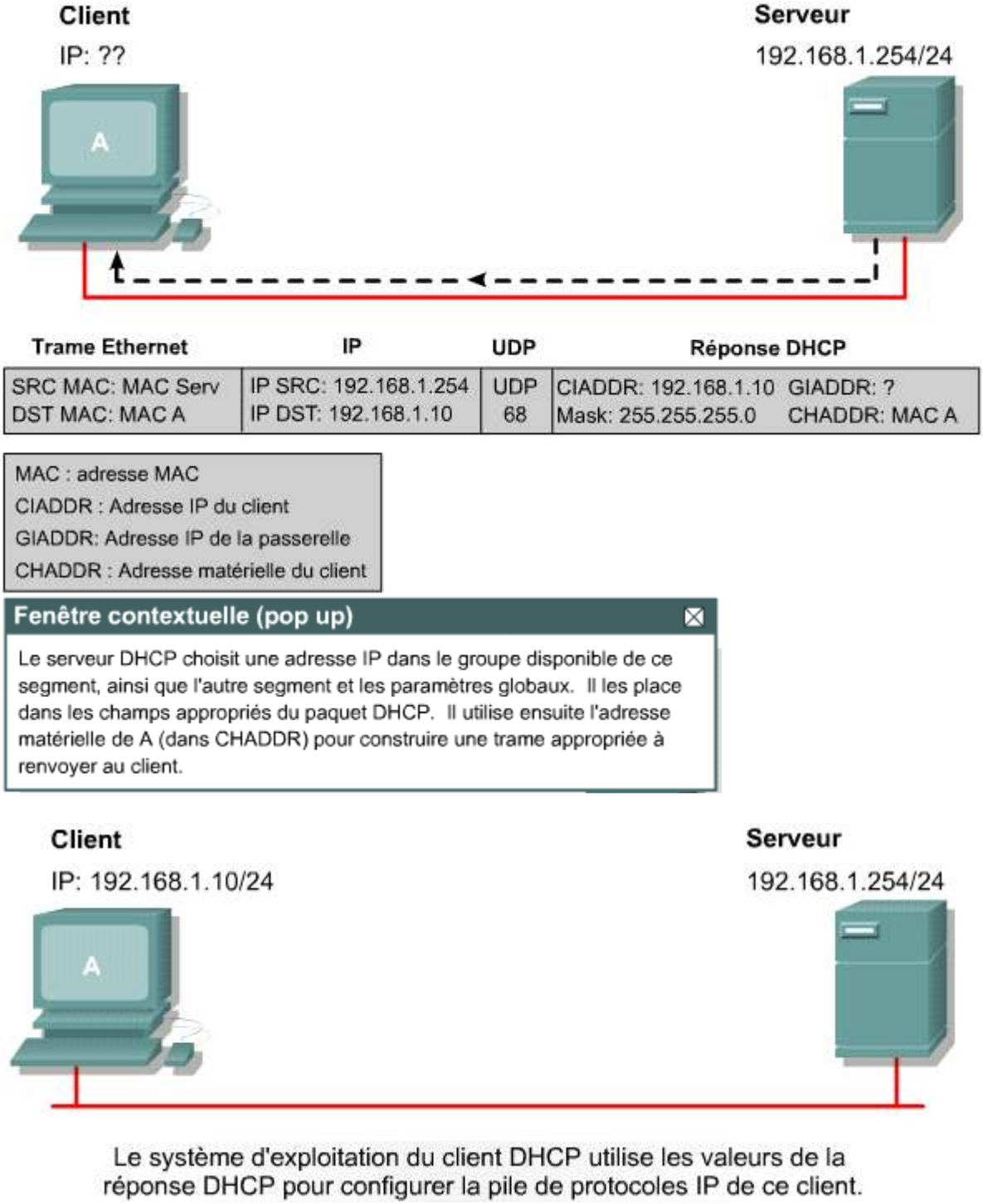
Trame Ethernet		IP	UDP	Requête DHCP	
SRC MAC: MAC A	DST MAC: FF:FF:FF:FF:FF:FF	IP SRC: ? IP DST: 255.255.255.255	UDP 67	CIADDR: ? Mask:?	GIADDR: ? CHADDR: MAC A

MAC : adresse MAC
CIADDR : Adresse IP du client
GIADDR: Adresse IP de la passerelle
CHADDR : Adresse matérielle du client

Fenêtre contextuelle (pop up)

Le client DHCP envoie un broadcast IP dirigé, avec un paquet de requête DHCP. Dans le cas le plus simple, il existe un serveur DHCP sur le même segment pour recueillir la requête. Le serveur note que le champ GIADDR est vide, ce qui signifie que le client est sur le même segment. Le serveur note également l'adresse matérielle du client dans le paquet de requête.

Ce serveur gère l'allocation des adresses IP et répond aux requêtes de configuration des clients. [2] [3]


Client
IP: ??
Serveur
192.168.1.254/24
A
Trame Ethernet
IP
UDP
Réponse DHCP
SRC MAC: MAC Serv
DST MAC: MAC A
IP SRC: 192.168.1.254
IP DST: 192.168.1.10
UDP
68
CIADDR: 192.168.1.10
Mask: 255.255.255.0
GIADDR: ?
CHADDR: MAC A
MAC : adresse MAC
CIADDR : Adresse IP du client
GIADDR: Adresse IP de la passerelle
CHADDR : Adresse matérielle du client
Fenêtre contextuelle (pop up)
Le serveur DHCP choisit une adresse IP dans le groupe disponible de ce segment, ainsi que l'autre segment et les paramètres globaux. Il les place dans les champs appropriés du paquet DHCP. Il utilise ensuite l'adresse matérielle de A (dans CHADDR) pour construire une trame appropriée à renvoyer au client.
Client
IP: 192.168.1.10/24
Serveur
192.168.1.254/24
A
Le système d'exploitation du client DHCP utilise les valeurs de la réponse DHCP pour configurer la pile de protocoles IP de ce client.

Le serveur DHCP peut répondre à des requêtes pour de nombreux sous-réseaux. Le protocole DHCP n'est pas destiné à configurer les routeurs, les commutateurs et les serveurs. Ces types d'hôtes nécessitent des adresses IP statiques.

Le protocole DHCP fonctionne en fournissant un processus permettant à un serveur d'allouer des informations IP à des clients. Les clients louent ces informations au serveur pour la période définie par l'administrateur. À l'expiration de la période d'utilisation, le client doit demander une autre adresse, même si l'adresse courante est généralement reconduite.

En règle générale, les administrateurs préfèrent qu'un serveur réseau fournisse des services DHCP, car ces solutions sont évolutives et relativement faciles à gérer. Les routeurs Cisco peuvent utiliser un jeu de fonctions Cisco IOS, Easy IP, pour offrir en option un serveur DHCP complet. Par défaut, Easy IP concède des configurations pendant 24 heures. Ceci s'avère utile dans les petits bureaux ou pour les télétravailleurs, qui peuvent ainsi profiter de DHCP et de NAT sans disposer d'un serveur Windows ou UNIX.

Les administrateurs configurent des serveurs DHCP pour assigner des adresses prises dans des groupes prédéfinis. Les serveurs DHCP peuvent également fournir d'autres informations, telles que des adresses de serveurs DNS, des adresses de serveurs WINS et des noms de domaine. La plupart des serveurs DHCP permettent aussi à l'administrateur de définir spécifiquement les adresses MAC des clients qui peuvent être desservis et de leur attribuer la même adresse IP à chaque fois. 1 2 3

Le protocole DHCP s'appuie sur le protocole de transport UDP (*User Datagram Protocol*). Le client envoie des messages au serveur sur le port 67. Le serveur envoie des messages au client sur le port 68.

1.2 Protocole DHCP

1.2.2 Différences entre les protocoles BOOTP et DHCP

La communauté Internet a tout d'abord développé le protocole BOOTP pour assurer la configuration des stations de travail sans disque. Le protocole BOOTP a été défini à l'origine dans la RFC 951 de 1985. En tant que prédécesseur de DHCP, BOOTP partage certaines de ses caractéristiques. Les deux protocoles sont de type client/serveur et utilisent les ports UDP 67 et 68. Ces ports continuent à s'appeler les ports BOOTP.

Les quatre paramètres IP de base sont:

- L'adresse IP
- L'adresse de passerelle
- Le masque de sous-réseau
- L'adresse du serveur DNS

Le protocole BOOTP n'attribue pas les adresses IP à un hôte de façon dynamique. Quand un client demande une adresse IP, le serveur BOOTP recherche dans une table prédéfinie l'entrée qui correspond à l'adresse MAC du client. S'il existe une entrée, l'adresse IP correspondante est renvoyée au client. Ceci signifie que la liaison entre l'adresse MAC et l'adresse IP doit déjà avoir été configurée dans le serveur BOOTP.

Il existe deux différences principales entre les protocoles DHCP et BOOTP: 1

BOOTP	DHCP
Mappages statiques	Mappages dynamiques
Assignation permanente	Bail
Ne prend en charge que quatre paramètres de configuration	Prend en charge plus de 30 paramètres de configuration

- DHCP définit des mécanismes par lesquels les clients peuvent se voir attribuer une adresse IP pendant une période d'utilisation déterminée. Cette période d'utilisation permet de réattribuer l'adresse IP à un autre client ou permet au client d'en obtenir une nouvelle s'il passe sur un autre sous-réseau. Les clients peuvent également renouveler les périodes d'utilisation et conserver la même adresse IP.
- Le protocole DHCP fournit le mécanisme permettant à un client de récupérer d'autres paramètres de configuration IP, telles que le WINS et le nom de domaine.

1.2 Protocole DHCP

1.2.3 Principales fonctions DHCP

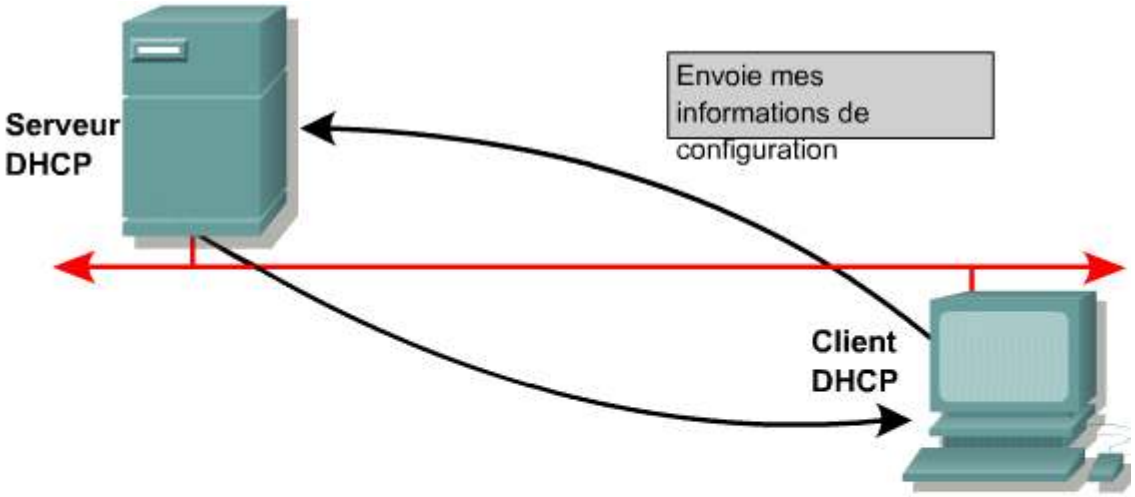
Trois mécanismes permettent d'attribuer une adresse IP au client:

- **L'allocation automatique** – Le protocole DHCP attribue une adresse IP permanente à un client.
- **L'allocation manuelle** – C'est l'administrateur qui attribue l'adresse IP au client. DHCP transfère l'adresse au client.
- **L'allocation dynamique** – DHCP attribue, ou concède, une adresse IP au client pendant une durée limitée.

La présente section concerne principalement le mécanisme d'allocation dynamique. Certains des paramètres de configuration disponibles sont énumérés dans l'IETF RFC 1533:

- Le masque de sous-réseau
- Le routeur
- Le nom de domaine
- Le(s) serveur(s) de noms de domaine
- Le(s) serveur(s) WINS

Le serveur DHCP crée des groupes d'adresses IP et leurs paramètres associés. 1 Les groupes sont dédiés à un sous-réseau IP logique individuel. Cela permet à plusieurs serveurs DHCP de répondre et aux clients IP d'être mobiles. Si plusieurs serveurs répondent, un client peut seulement choisir l'une des offres.

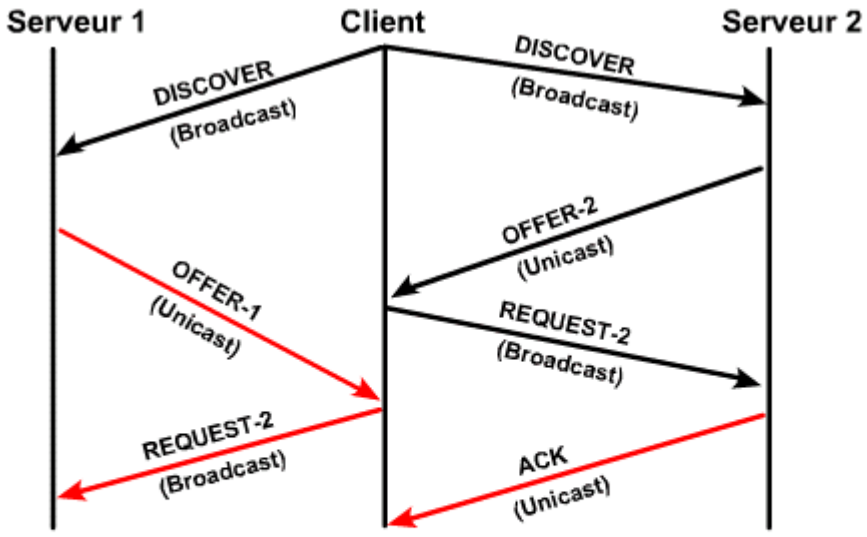


Voici votre configuration :
- IP Address: 192.204.18.7
- Subnet Mask: 255.255.255.0
- Default Routers: 192.204.18.1, 192.204.18.3
- DNS Servers: 192.204.18.8, 192.204.18.9
- Lease Time: 5 days

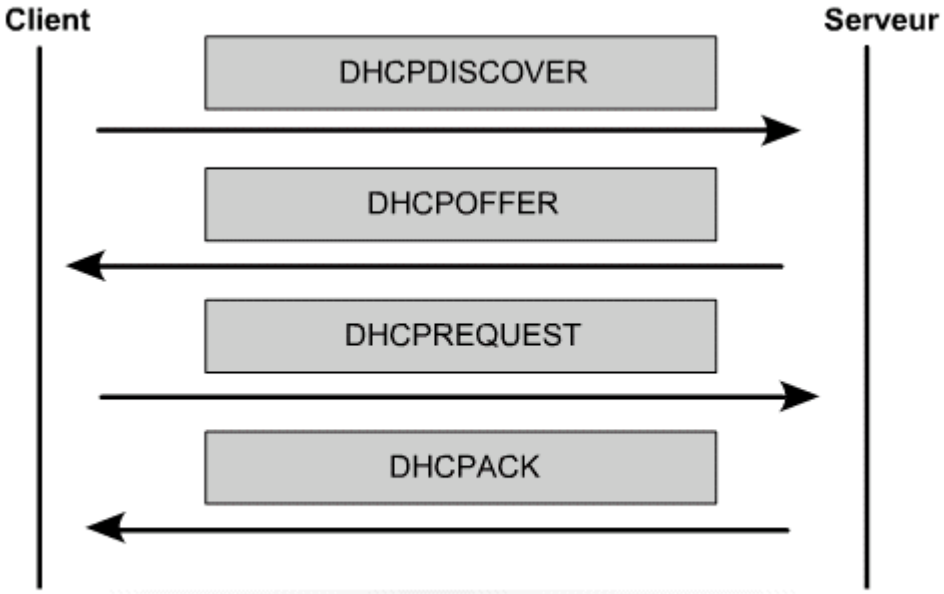
1.2 Protocole DHCP

1.2.4 Fonctionnement du protocole DHCP

Le processus de configuration du client DHCP se déroule comme suit: 1 2



- Le client DHCP envoie par broadcast un paquet DHCPDISCOVER sur le sous-réseau local
- Les serveurs DHCP envoient un paquet OFFER avec des informations de bail
- Le client DHCP sélectionne le bail et envoie par broadcast un paquet DHCPREQUEST
- Le serveur DHCP sélectionné envoie un paquet DHCPACK



Les messages DHCP dans leur ordre de transmission

1. DHCP doit être configuré sur un client au début du processus d'appartenance au réseau. Le client envoie une requête de configuration IP à un serveur. Il peut arriver que le client suggère l'adresse IP dont il a besoin, par exemple pour demander l'extension d'une période d'utilisation de DHCP. Le client localise un serveur DHCP en envoyant un broadcast dénommé DHCPDISCOVER.
2. Quand le serveur reçoit le broadcast, il détermine s'il peut desservir la requête à partir de sa propre base de données. Quand il n'y parvient pas, le serveur peut transférer la requête à un autre serveur DHCP. S'il y parvient, le serveur DHCP offre au client les informations de configuration IP sous la forme d'un DHCPOFFER unicast. Le DHCPOFFER est une configuration proposée qui peut inclure une adresse IP, une adresse de serveur DNS et la durée d'utilisation.
3. Si l'offre convient au client, celui-ci envoie un autre broadcast, DHCPREQUEST, pour demander spécifiquement ces paramètres IP. Pourquoi est-ce que le client effectue la requête par broadcast et non par unicast vers le serveur ? C'est un broadcast qui est utilisé parce que le premier message, à savoir DHCPDISCOVER, peut être parvenu à plusieurs serveurs DHCP. Si plusieurs serveurs renvoient une offre, le DHCPREQUEST diffusé en broadcast permet aux autres serveurs de savoir quelle offre a été acceptée. L'offre acceptée est généralement la première reçue.
4. Le serveur qui reçoit la demande DHCPREQUEST officialise la configuration en envoyant un accusé de réception en unicast, le DHCPACK. Il est possible, mais hautement improbable, que le serveur n'envoie pas le DHCPACK. Ceci peut se produire si le serveur a concédé ces informations à un autre client entre temps. Dès qu'il reçoit le message DHCPACK, le client peut commencer à utiliser l'adresse attribuée.
5. Si le client détecte que l'adresse est en cours d'utilisation sur le segment local, il envoie un message DHCPDECLINE et le processus recommence. Si le client a reçu un DHCPNACK du serveur après avoir envoyé le DHCPREQUEST, il recommence tout le processus.
6. Si le client n'a plus besoin de l'adresse IP, il envoie un message DHCPRELEASE au serveur.

En fonction des politiques d'une entreprise, il est possible à un utilisateur de base ou à un administrateur d'assigner à un hôte de façon statique une adresse IP appartenant au groupe d'adresses du serveur DHCP. Par sécurité, le serveur IOS DHCP Cisco s'assure toujours que l'adresse n'est pas utilisée avant de la proposer à un client. Le serveur émet une requête d'écho ICMP ou un ping vers une adresse du groupe avant d'envoyer le message DHCPOFFER à un client. Bien qu'il puisse être configuré, le nombre par défaut de pings utilisés pour vérifier une adresse IP potentielle s'élève à deux.

1.2 Protocole DHCP

1.2.5 Configuration de DHCP

À l'instar de la fonction NAT, un serveur DHCP nécessite que l'administrateur ait défini un groupe d'adresses. La commande **`ip dhcp pool`** définit les adresses qui vont être attribuées aux hôtes.

La première commande, **`ip dhcp pool`**, crée un groupe portant le nom spécifié, puis place le routeur en mode spécialisé de configuration DHCP. Dans ce mode, utilisez l'instruction **`network`** pour définir la plage d'adresses à octroyer. 1 Si des adresses spécifiques du réseau doivent être exclues, revenez au mode de configuration globale.

```
Router(config)#ip dhcp pool pool-name
```

Spécifie le groupe DHCP

```
Router(dhcp-config)#network network-number [mask|/prefix-length]
```

Spécifie la plage d'adresses du groupe

- Crée un groupe DHCP IP et lui attribue un nom
- Plusieurs groupes DHCP peuvent être créés sur un seul serveur
- Spécifie la plage d'adresses IP avec une adresse de réseau IP et un masque

La commande **ip dhcp excluded-address** configure le routeur pour lui faire exclure une adresse ou une série d'adresses lors de l'assignation d'adresses à des clients. La commande **ip dhcp excluded-address** peut être utilisée pour réserver des adresses attribuées de façon statique à des hôtes clés, par exemple l'adresse d'interface sur le routeur. 2

```
Router(config)#ip dhcp excluded-address low-address [high-address]
```

```
Router(config)#ip dhcp excluded-address 172.16.1.1 172.16.1.10
Router(config)#ip dhcp excluded-address 172.16.1.254
```

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

En règle générale, la configuration d'un serveur DHCP lui permet d'attribuer beaucoup plus qu'une adresse IP. D'autres valeurs de configuration IP, telles que la passerelle par défaut, peuvent être définies à partir du mode de configuration de DHCP. La commande **default-router** définit la passerelle par défaut. Les adresses du serveur DNS, **dns-server**, et du serveur WINS, **netbios-name-server**, peuvent également être configurées ici. Le serveur IOS DHCP peut configurer des clients avec pratiquement n'importe quelles informations TCP/IP.

La liste des principales commandes du serveur IOS DHCP entrées dans le mode de configuration du groupe DHCP est présentée à la figure 3.

Commande	Description
network *network-number* [*mask* | */prefix-length*]	Spécifie le numéro de sous-réseau et le masque du groupe d'adresses DHCP. La longueur du préfixe spécifie le nombre de bits qui constituent le préfixe de l'adresse. Le préfixe constitue une autre manière de spécifier le masque de réseau du client. La longueur du préfixe doit être précédée d'une barre oblique (/).
default-router *address* [*address2...address8*]	Spécifie l'adresse IP de la passerelle par défaut pour un client DHCP. Bien qu'une seule adresse soit requise, il est possible d'en spécifier jusqu'à huit dans une ligne de commande.
dns-server *address* [*address2...address8*]	Spécifie l'adresse IP d'un serveur DNS à la disposition d'un client DHCP. Bien qu'une seule adresse soit requise, il est possible d'en spécifier jusqu'à huit dans une ligne de commande.
netbios-name-server *address* [*address2...address8*]	Spécifie le serveur NetBios WINS à la disposition d'un client DHCP Microsoft. Bien qu'une seule adresse soit requise, il est possible d'en spécifier jusqu'à huit dans une ligne de commande.
domain-name *name*	Spécifie le nom de domaine pour le client.
lease {*days* [*hours*] [*minutes*] | infinite}	Spécifie la durée du bail. Par défaut, le bail dure une journée.

Le service DHCP est activé par défaut sur les versions de Cisco IOS qui le prennent en charge. Pour désactiver le service, utilisez la commande **no service dhcp**. Utilisez la commande de configuration globale **service dhcp** pour réactiver le processus du serveur DHCP.

1.2 Protocole DHCP

1.2.6 Vérification du fonctionnement du protocole DHCP

Pour vous assurer du bon fonctionnement du protocole DHCP, vous pouvez utiliser la commande **show ip dhcp binding**. Elle affiche la liste de toutes les liaisons créées par le service DHCP. 1

```
Router#show ip dhcp binding
```

```
Router#show ip dhcp binding
IP address      Hardware address    Lease expiration      Type
172.16.12.11    0100.10a4.97f4.6d   Mar 02 1993 12:38 AM  Automatic
Router#
```

Pour vous assurer que des messages sont reçus ou envoyés par le routeur, utilisez la commande **show ip dhcp server statistics**. Elle fournit les nombres de messages DHCP envoyés et reçus.

Activité de TP

Exercice: Configuration de DHCP

Au cours de ce TP, l'étudiant va configurer un routeur pour le protocole DHCP (*Dynamic Host Configuration Protocol*).

Activité de TP

Activité en ligne: Configuration de DHCP

Au cours de ce TP, l'étudiant va configurer un routeur pour le protocole DHCP, ajouter une fonctionnalité permettant aux stations de travail d'obtenir à distance des adresses DHCP et attribuer de façon dynamique des adresses aux hôtes rattachés.

1.2.7 Dépannage du protocole DHCP

Pour dépanner le protocole DHCP, vous pouvez utiliser la commande **debug ip dhcp server events**. Cette commande montre que le serveur vérifie régulièrement si les périodes d'utilisation ont expiré. S'affichent également les processus des adresses renvoyées et des adresses allouées. 1

```
Router#debug ip dhcp server events
```

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

1.2 Protocole DHCP

1.2.8 Relais DHCP

Les clients DHCP utilisent des broadcasts IP pour retrouver le serveur DHCP sur le segment. Que se passe-t-il quand le serveur et le client ne résident pas sur le même segment et sont séparés par un routeur ? Les routeurs ne transmettent pas les broadcasts.

DHCP n'est pas le seul service critique à faire appel aux broadcasts. Les routeurs Cisco et d'autres équipements peuvent utiliser des broadcasts pour localiser les serveurs TFTP. Certains clients peuvent avoir besoin d'émettre un broadcast pour localiser un serveur TACACS. Un serveur TACACS est un serveur de sécurité. Généralement, sur un réseau hiérarchique complexe, les clients résident sur le même sous-réseau que les serveurs clés. Ces clients distants émettent des broadcasts pour localiser ces serveurs. En revanche, par défaut, les routeurs ne transfèrent aucun message de broadcast au-delà de leur propre sous-réseau.

Comme certains clients sont inutiles sans des services comme DHCP, l'administrateur doit choisir entre les deux options suivantes : placer des serveurs sur tous les sous-réseaux ou utiliser la fonction adresse de diffusion de Cisco IOS. Le fait d'exécuter des services tels que DHCP ou DNS sur plusieurs ordinateurs est à l'origine de surcharges et de difficultés administratives, lesquelles rendent la première option inefficace. Lorsque c'est possible, les administrateurs doivent utiliser la commande **ip helper-address** pour relayer les requêtes de broadcast pour ces services UDP clés.

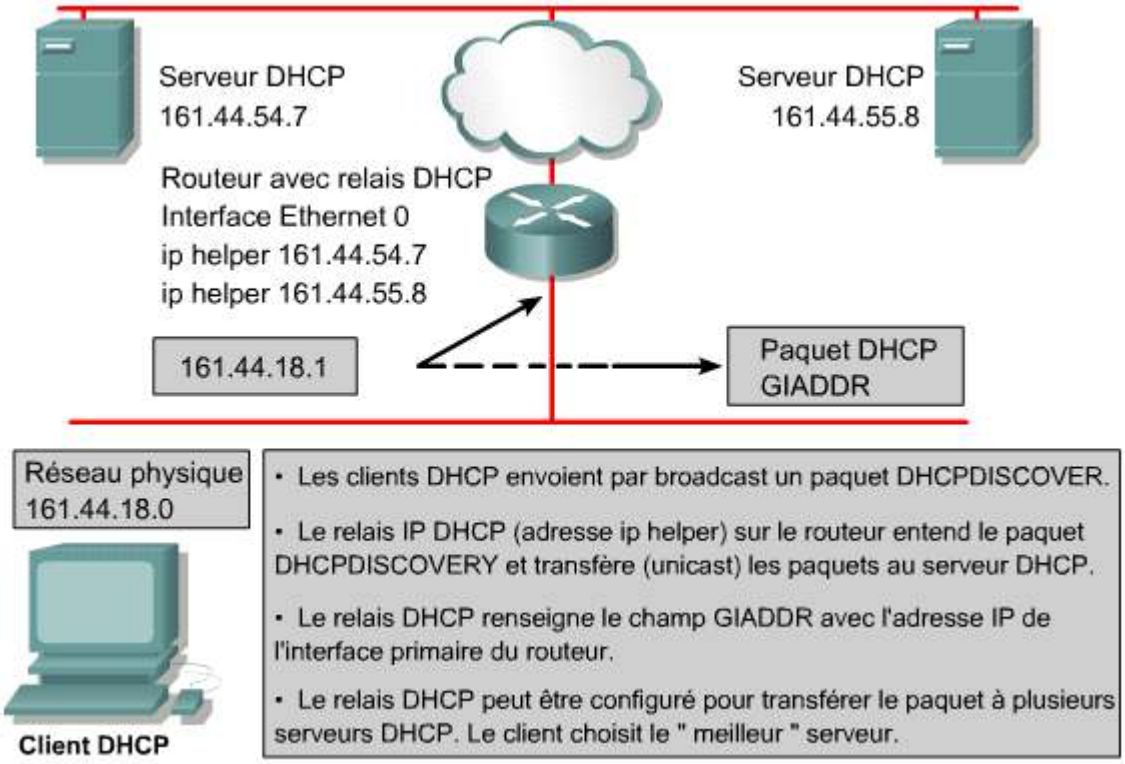
En utilisant la fonction d'adresse de diffusion, il est possible de configurer un routeur pour lui faire accepter une requête de broadcast de service UDP, puis de la transférer en unicast vers une adresse IP spécifique. Par défaut, la commande **ip helper-address** transfère les huit services UDP suivants:

- Protocole Time
- TACACS
- Le protocole DNS
- Le serveur BOOTP/DHCP
- Le client BOOTP/DHCP
- TFTP
- Le service de noms NetBIOS
- Le service de datagramme NetBIOS

Dans le cas particulier de DHCP, un client diffuse un paquet DHCPDISCOVER sur son segment local. 1

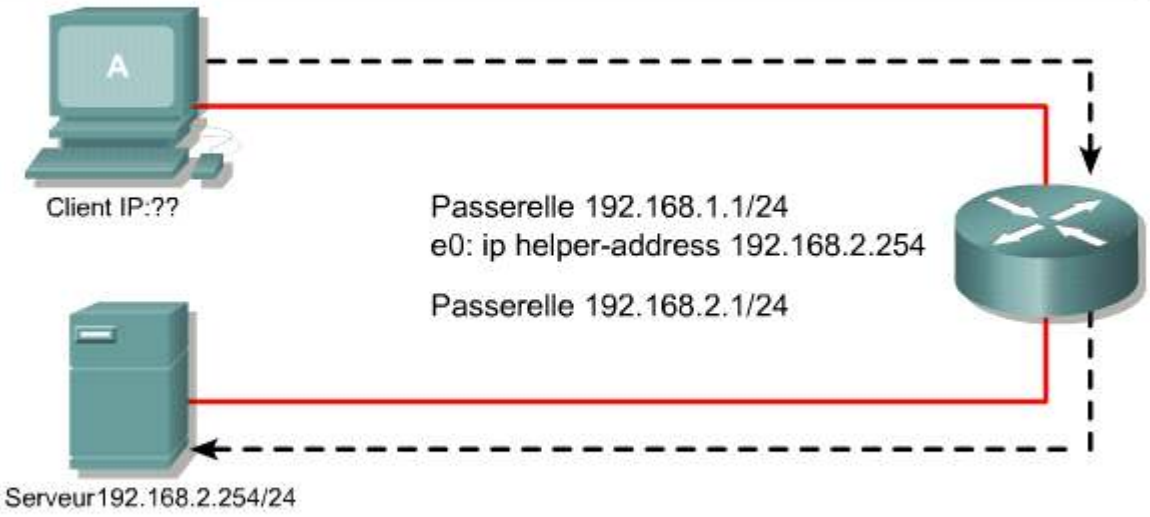
Code OP - 1 octet	Type de matériel - 1 octet	Longueur matériel - 1 octet	Sauts - 1 octet
ID transaction ID (XID) - 4 octets			
Secondes - 2 octets		Indicateurs - 2 octets	
Adresse IP client (CIADDR) - 4 octets			
Votre adresse IP (YIADDR) - 4 octets			
Adresse IP serveur (SIADDR) - 4 octets			
Adresse IP passerelle (GIADDR) - 4 octets			
Adresse matérielle client (CHADDR) -16 octets			
Nom serveur (SNAME) - 64 octets			
Nom de fichier - 128 octets			
Options DHCP - 312 octets			

Ce paquet est prélevé par la passerelle. Si une adresse de diffusion est configurée, le paquet DHCP est transféré à l'adresse spécifiée. Avant de transférer le paquet, le routeur renseigne le champ GIADDR du paquet avec l'adresse IP du routeur de ce segment. Cette adresse représente ensuite l'adresse de passerelle pour le client DHCP lorsque celui-ci obtient l'adresse IP. 2


Serveur DHCP
161.44.54.7
Serveur DHCP
161.44.55.8
Routeur avec relais DHCP
Interface Ethernet 0
ip helper 161.44.54.7
ip helper 161.44.55.8
161.44.18.1
Paquet DHCP
GIADDR
Réseau physique
161.44.18.0
Client DHCP
• Les clients DHCP envoient par broadcast un paquet DHCPDISCOVER.
• Le relais IP DHCP (adresse ip helper) sur le routeur entend le paquet DHCPDISCOVERY et transfère (unicast) les paquets au serveur DHCP.
• Le relais DHCP renseigne le champ GIADDR avec l'adresse IP de l'interface primaire du routeur.
• Le relais DHCP peut être configuré pour transférer le paquet à plusieurs serveurs DHCP. Le client choisit le " meilleur " serveur.

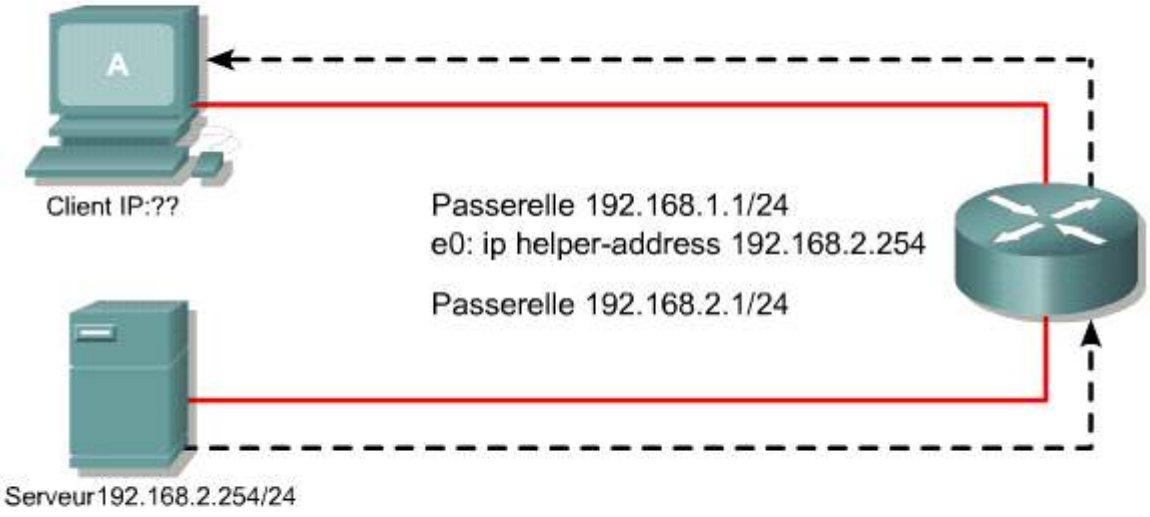
Le serveur DHCP reçoit le paquet de découverte. Le serveur utilise ensuite le champ GIADDR pour indexer la liste de groupes d'adresses afin d'en trouver un dont l'adresse de passerelle est configurée sur la valeur de GIADDR. Ce groupe est ensuite utilisé pour fournir son adresse IP au client. 3 – 4

Trame Ethernet broadcast	IP	UDP	Requête DHCP
SRC MAC: MAC A DST MAC: FF:FF:FF:FF:FF:FF	IP SRC? IP DST: 255.255.255.255	UDP 67	CIADDR: ? GIADDR: ? Mask: ? CHADDR: MAC A



Trame Ethernet unicast	IP	UDP	Requête DHCP
SRC MAC: MAC Passerelle DST MAC: MAC Serv	IP SRC: 192.168.2.1 IP DST: 192.168.2.254	UDP 67	CIADDR: ? GIADDR: 192.168.1.1 Mask: ? CHADDR: MAC A

Trame Ethernet unicast	IP	UDP	Réponse DHCP
SRC MAC: MAC Passerelle DST MAC: MAC A	IP SRC: 192.168.2.254 IP DST: 192.168.1.10	UDP 68	GIADDR: 192.168.1.1 CHADDR: MAC A Mask: 255.255.255.0 CIADDR: 192.168.1.10



Trame Ethernet unicast	IP	UDP	Réponse DHCP
SRC MAC: MAC Serv DST MAC: MAC Passerelle	IP SRC: 192.168.2.254 IP DST: 192.168.1.10	UDP 68	GIADDR: 192.168.1.1 CHADDR: MAC A Mask: 255.255.255.0 CIADDR: 192.168.1.10

Activité de TP

Exercice: Configuration du relais DHCP

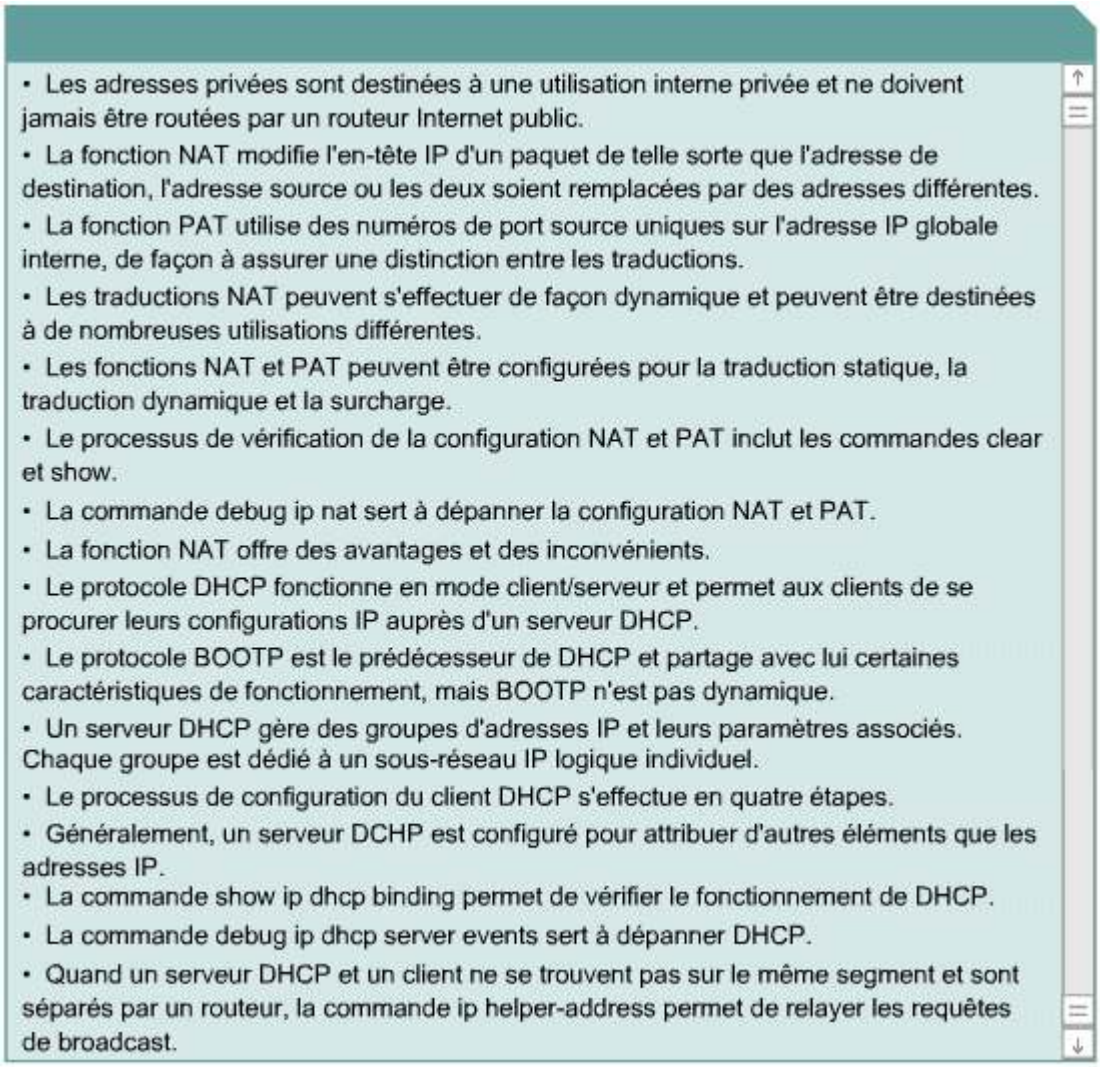
Au cours de ce TP, un routeur va être configuré pour le protocole DHCP (*Dynamic Host Configuration Protocol*).

Activité de TP

Activité en ligne: Configuration du relais DHCP. Au cours de ce TP, l'étudiant va configurer un routeur pour le protocole DHCP, ajouter une fonctionnalité permettant aux stations de travail d'obtenir à distance des adresses DHCP et attribuer de façon dynamique des adresses aux hôtes rattachés.

RésuméLa compréhension des points clés suivants devrait être acquise:

- Les adresses privées sont destinées à une utilisation interne privée et ne doivent jamais être routées par un routeur Internet public.
- La fonction NAT modifie l'en-tête IP d'un paquet de telle sorte que l'adresse de destination, l'adresse source ou les deux soient remplacées par des adresses différentes.
- La fonction PAT utilise des numéros de port source uniques sur l'adresse IP globale interne, de façon à assurer une distinction entre les traductions.
- Les traductions NAT peuvent s'effectuer de façon dynamique et peuvent être destinées à de nombreuses utilisations différentes.
- Les fonctions NAT et PAT peuvent être configurées pour la traduction statique, la traduction dynamique et la surcharge.
- Le processus de vérification de la configuration NAT et PAT inclut les commandes **`clear`** et **`show`**.
- La commande **`debug ip nat`** sert à dépanner la configuration NAT et PAT.
- La fonction NAT offre des avantages et des inconvénients.
- Le protocole DHCP fonctionne en mode client/serveur et permet aux clients de se procurer leurs configurations IP auprès d'un serveur DHCP.
- Le protocole BOOTP est le prédécesseur de DHCP et partage avec lui certaines caractéristiques de fonctionnement, mais BOOTP n'est pas dynamique.
- Un serveur DHCP gère des groupes d'adresses IP et leurs paramètres associés. Chaque groupe est dédié à un sous-réseau IP logique individuel.
- Le processus de configuration du client DHCP s'effectue en quatre étapes.
- Généralement, un serveur DCHP est configuré pour attribuer d'autres éléments que les adresses IP.
- La commande **`show ip dhcp binding`** permet de vérifier le fonctionnement du protocole DHCP.
- La commande **`debug ip dhcp server events`** permet de dépanner le protocole DHCP.
- Quand un serveur DHCP et un client ne se trouvent pas sur le même segment et sont séparés par un routeur, la commande **`ip helper-address`** permet de relayer les requêtes de broadcast.


• Les adresses privées sont destinées à une utilisation interne privée et ne doivent jamais être routées par un routeur Internet public.
• La fonction NAT modifie l'en-tête IP d'un paquet de telle sorte que l'adresse de destination, l'adresse source ou les deux soient remplacées par des adresses différentes.
• La fonction PAT utilise des numéros de port source uniques sur l'adresse IP globale interne, de façon à assurer une distinction entre les traductions.
• Les traductions NAT peuvent s'effectuer de façon dynamique et peuvent être destinées à de nombreuses utilisations différentes.
• Les fonctions NAT et PAT peuvent être configurées pour la traduction statique, la traduction dynamique et la surcharge.
• Le processus de vérification de la configuration NAT et PAT inclut les commandes clear et show.
• La commande debug ip nat sert à dépanner la configuration NAT et PAT.
• La fonction NAT offre des avantages et des inconvénients.
• Le protocole DHCP fonctionne en mode client/serveur et permet aux clients de se procurer leurs configurations IP auprès d'un serveur DHCP.
• Le protocole BOOTP est le prédécesseur de DHCP et partage avec lui certaines caractéristiques de fonctionnement, mais BOOTP n'est pas dynamique.
• Un serveur DHCP gère des groupes d'adresses IP et leurs paramètres associés. Chaque groupe est dédié à un sous-réseau IP logique individuel.
• Le processus de configuration du client DHCP s'effectue en quatre étapes.
• Généralement, un serveur DCHP est configuré pour attribuer d'autres éléments que les adresses IP.
• La commande show ip dhcp binding permet de vérifier le fonctionnement de DHCP.
• La commande debug ip dhcp server events sert à dépanner DHCP.
• Quand un serveur DHCP et un client ne se trouvent pas sur le même segment et sont séparés par un routeur, la commande ip helper-address permet de relayer les requêtes de broadcast.

Vue d'ensemble

À mesure que l'entreprise s'étend au-delà d'un seul local, il s'avère nécessaire d'interconnecter les LAN des diverses filiales pour constituer un réseau étendu (WAN – *Wide Area Network*). Ce module examine les options disponibles pour ces interconnexions, le matériel nécessaire à leur mise en oeuvre et la terminologie utilisée pour les désigner.

De nos jours, de nombreuses options sont disponibles pour mettre en œuvre des solutions WAN. Elles diffèrent au niveau de la technologie, de la vitesse et du coût. Il est important d'être familier avec ces technologies pour une bonne conception et une bonne évaluation du réseau.

Si tout le trafic de données d'une entreprise est regroupé dans un seul bâtiment, un réseau LAN suffit aux besoins de celle-ci. Les bâtiments peuvent être interconnectés par des liaisons haut débit pour constituer un réseau LAN de complexe si les données doivent passer de l'un des bâtiments du complexe à l'autre. En revanche, un réseau WAN s'avère nécessaire pour transporter les données si celles-ci doivent être transférées entre des sites séparés géographiquement. L'accès à distance individuel au réseau local et la connexion de ce dernier à Internet constituent des sujets distincts, qui ne seront pas étudiés ici.

La plupart des étudiants ne vont pas avoir l'opportunité de concevoir de nouveaux réseaux WAN, mais vont être impliqués dans la conception d'extensions et de mises à niveaux pour des WAN existants en appliquant les techniques apprises dans le présent module.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

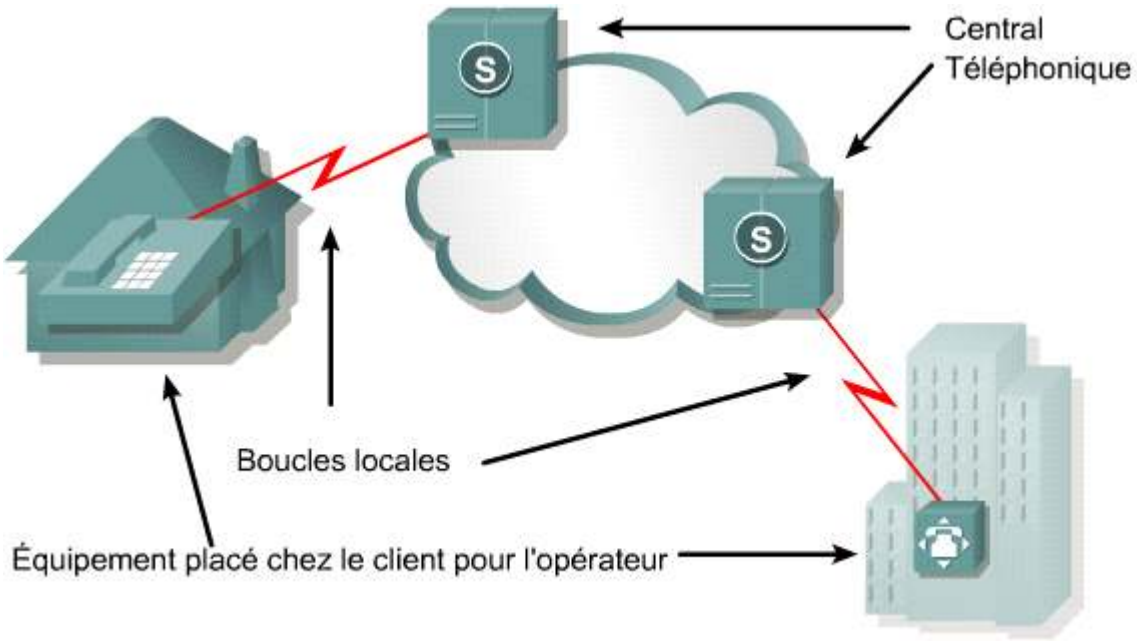
- Savoir différencier un réseau LAN d'un réseau WAN
- Identifier les équipements utilisés dans un réseau WAN
- Énumérer les normes liées aux WAN
- Décrire l'encapsulation WAN
- Classifier les diverses options de liaison WAN
- Savoir différencier les technologies WAN à commutation de paquets et à commutation de circuits
- Comparer les technologies WAN actuelles
- Décrire les équipements impliqués dans la mise en oeuvre de divers services de WAN
- Recommander un service de WAN à une entreprise en fonction des besoins de celle-ci
- Décrire les bases de la connectivité DSL et modem câble
- Décrire une procédure méthodique de désignation des WAN
- Comparer les topologies WAN
- Comparer les modèles de conception WAN
- Recommander une conception de réseau WAN à une entreprise en fonction des besoins de celle-ci

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
2.1	Aperçu des technologies WAN
2.2	Technologies WAN
2.3	Conception d'un WAN

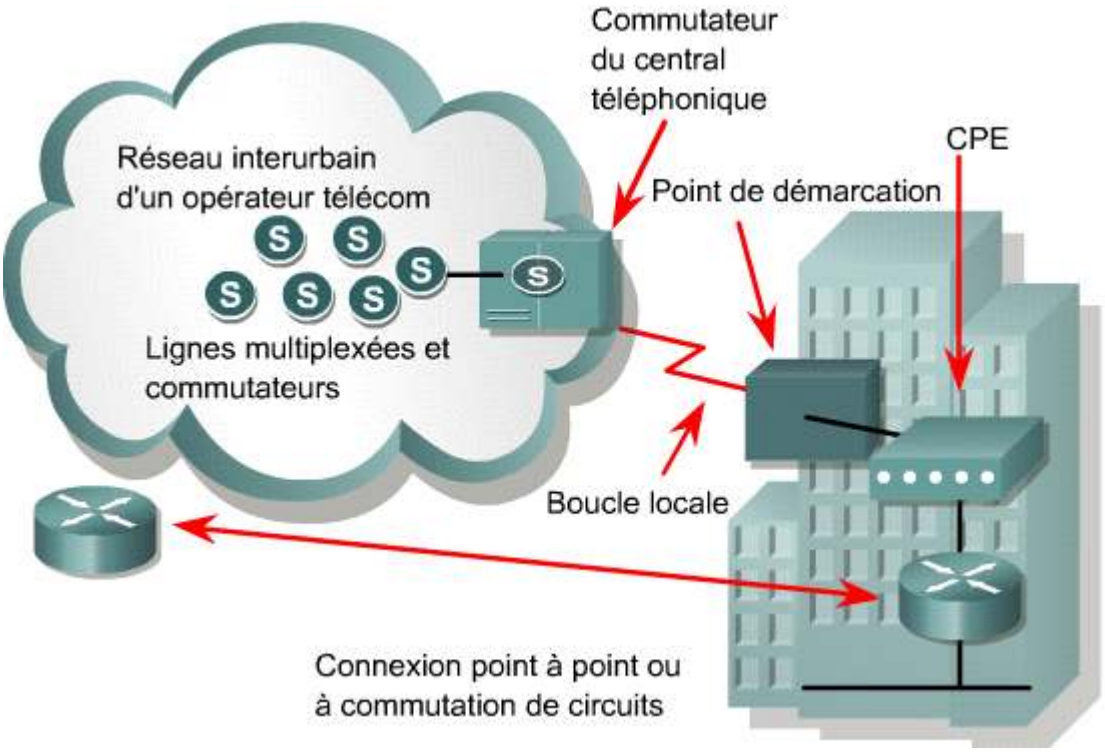
2.1 Aperçu des technologies WAN

2.1.1 Technologie WAN

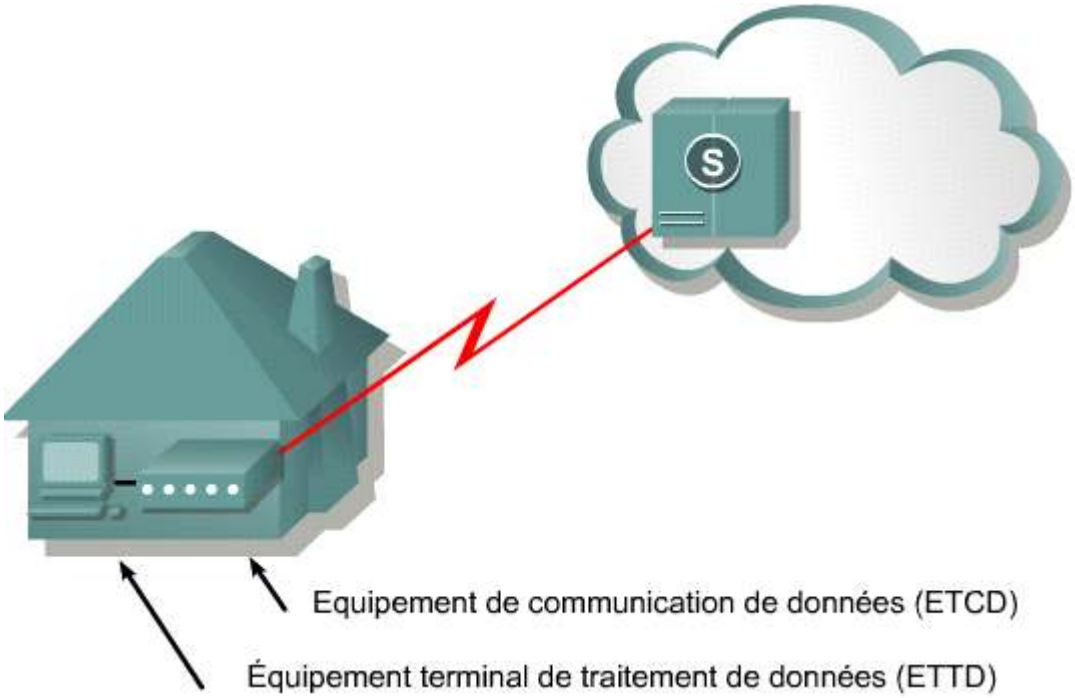
Un réseau WAN est un réseau de communication de données qui fonctionne au-delà de la portée géographique d'un réseau LAN. Les réseaux WAN et LAN ont pour différence principale qu'une société ou une entreprise doit s'abonner à un fournisseur d'accès WAN extérieur pour utiliser les services de réseau d'un opérateur WAN. Un réseau WAN utilise les liaisons de données fournies par un opérateur pour accéder à Internet et connecter les sites d'une entreprise entre eux, à des sites d'autres entreprises, à des services externes et à des utilisateurs distants. Les WAN transportent généralement divers types de trafic, tels que la voix, des données et des images vidéo. Les services de réseau WAN les plus couramment utilisés sont les services téléphoniques et de données.



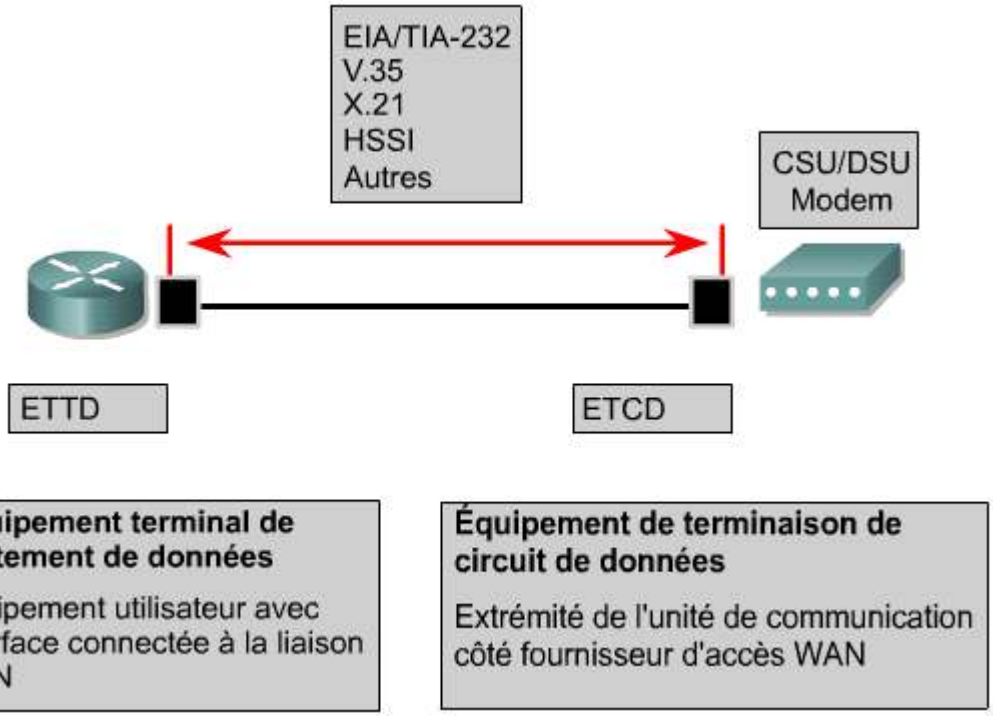
L'équipement situé dans les locaux de l'abonné est désigné par l'acronyme CPE (*customer premises equipment* – équipement placé chez le client pour l'opérateur). 1 L'abonné est propriétaire du CPE ou le loue à son fournisseur d'accès. Un câble en cuivre ou en fibres connecte le CPE au central d'échange ou téléphonique (CO – *central office*) le plus proche du fournisseur d'accès. Ce câblage est souvent désigné par le nom boucle locale. Un appel est connecté localement à d'autres boucles locales, ou non localement par l'intermédiaire d'une ligne multiplexée vers un central primaire. Il passe ensuite sur un central de section, puis un central d'opérateur régional ou international à mesure qu'il est mené à sa destination. 2



Pour que la boucle locale puisse transporter des données, un équipement tel qu'un modem s'avère nécessaire pour préparer la transmission. Les équipements qui mettent les données sur la boucle locale sont dénommées équipements de terminaison de circuit de données (ETCD) ou équipements de communication de données. Les équipements qui transmettent les données à l'ETCD sont appelés les équipements terminaux de traitement de données (ETTD). 3



L'ETCD sert essentiellement d'interface entre l'ETTD et la liaison de communication située dans le nuage du réseau WAN. L'interface ETCD/ETTD utilise diverses protocoles de couche physique, tels que l'interface HSSI (*High-Speed Serial Interface*) et V.35. Ces protocoles établissent les codes et les paramètres électriques que les équipements utilisent pour communiquer entre eux. 4



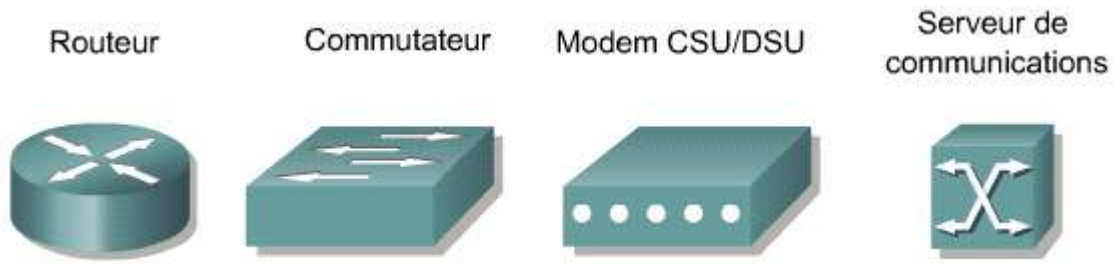
Les liaisons WAN existent à diverses vitesses, mesurées en bits par seconde (bits/s), kilobits par seconde (kbits/s ou 1000 bits/s), mégabits par seconde (Mbits/s ou 1000 kbits/s) ou gigabits par seconde (Gbits/s ou 1000 Mbits/s). Les valeurs en bits/s fonctionnent généralement en mode full duplex. Ceci signifie qu'une ligne E1 peut transporter 2 Mbits/s ou qu'une T1 peut en transporter 1,5 simultanément dans chaque direction. 5

Type de ligne	Norme de signal	Débit binaire
56	DS0	56 Kbits/s
64	DS0	64 Kbits/s
T1	DS1	1.544 Mbits/s
E1	ZM	2.048 Mbits/s
E3	M3	34.064 Mbits/s
J1	Y1	2.048 Mbits/s
T3	DS3	44.736 Mbits/s
OC-1	SONET	51.84 Mbits/s
OC-3	SONET	155.54 Mbits/s
OC-9	SONET	466.56 Mbits/s
OC-12	SONET	622.08 Mbits/s
OC-18	SONET	933.12 Mbits/s
OC-24	SONET	1244.16 Mbits/s
OC-36	SONET	1866.24 Mbits/s
OC-48	SONET	2488.32 Mbits/s

2.1 Aperçu des technologies WAN

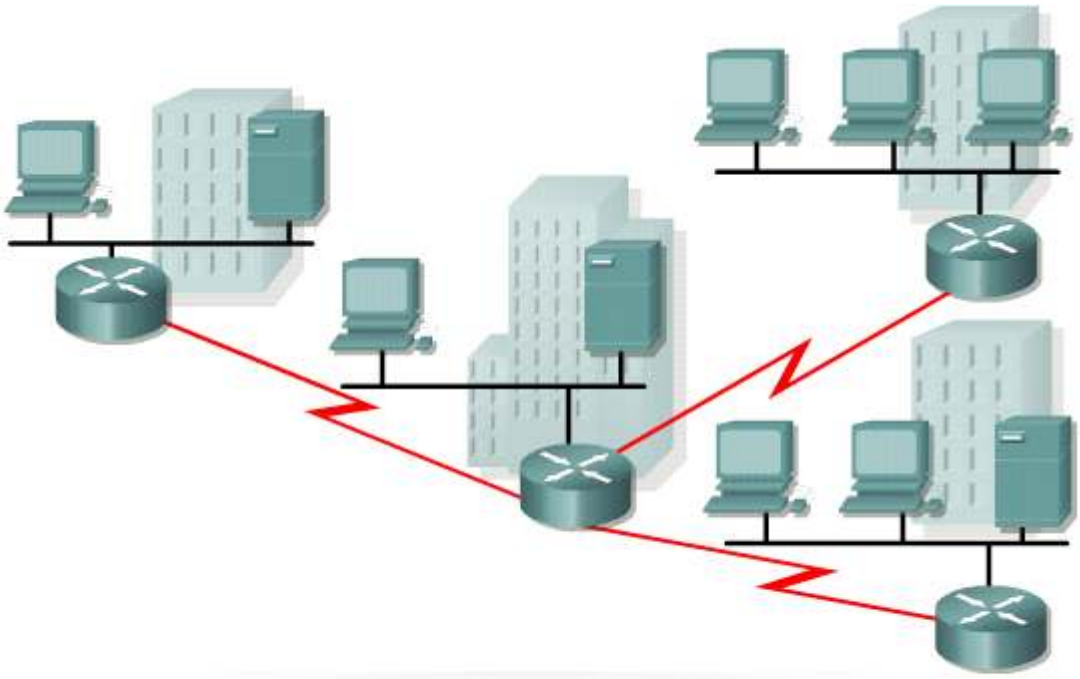
2.1.2 Équipements WAN

Les réseaux WAN sont des groupes de réseaux locaux connectés par des liaisons de communications fournies par un fournisseur d'accès. Comme ces liaisons de communications ne peuvent pas se connecter directement au réseau LAN, il est nécessaire d'identifier les divers éléments de l'équipement d'interfaçage. 1



Les réseaux WAN présentent les caractéristiques suivantes :
- Couvrent une vaste région géographique
- Permettent l'accès par des interfaces série plus lentes
- Assurent une connectivité continue ou intermittente

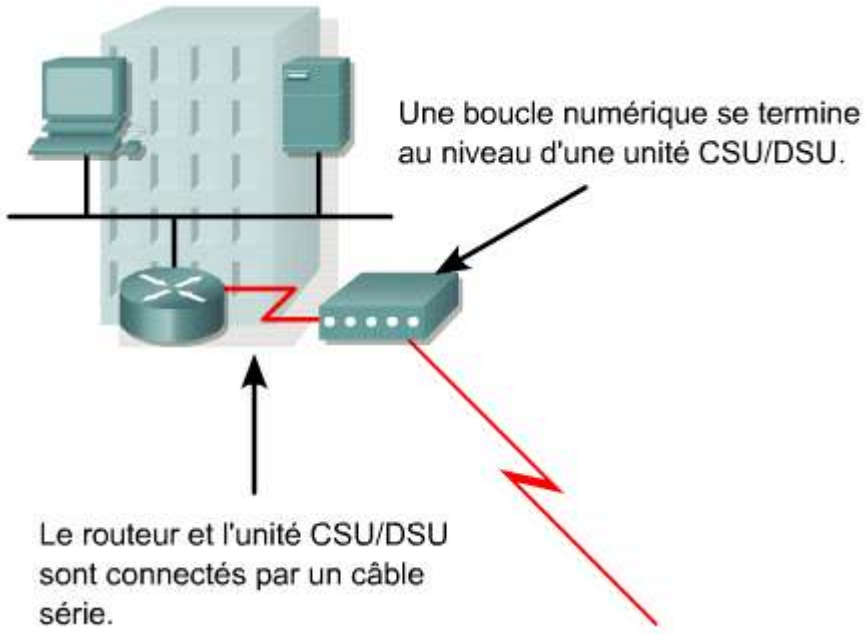
Les ordinateurs d'un réseau local ayant des données à transmettre les envoient sur un routeur qui contient à la fois des interfaces LAN et des interfaces WAN. 2



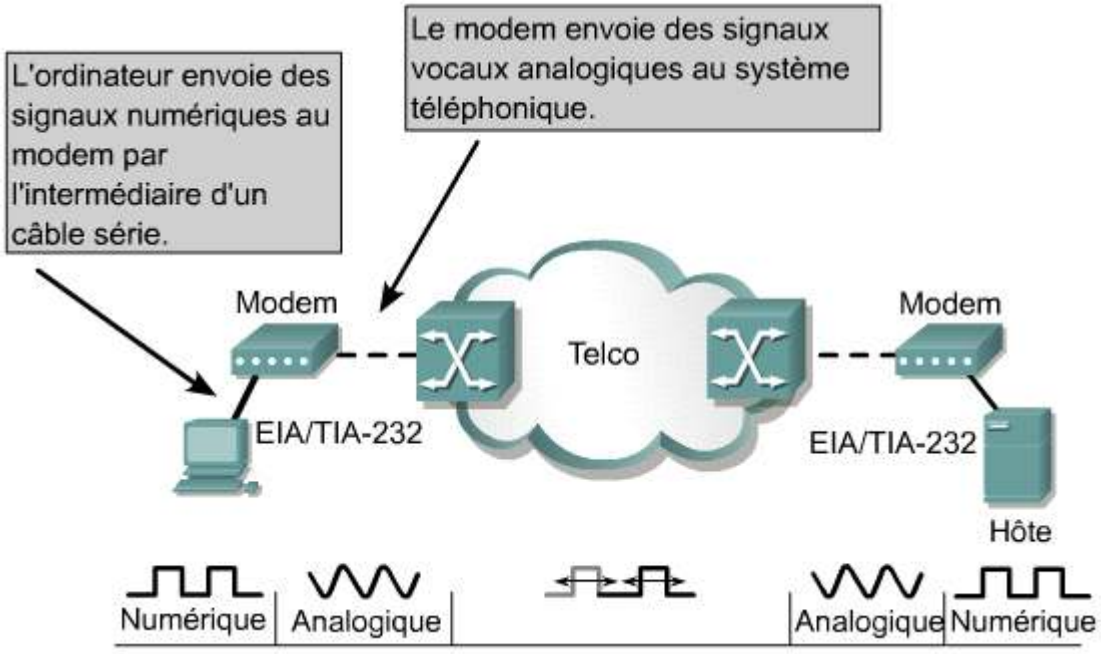
Plusieurs réseaux locaux sont connectés pour constituer un WAN. Les routeurs sont le point de connexion, qui s'interface avec le réseau local et le réseau WAN.

Le routeur utilise les informations d'adresse de couche 3 pour remettre les données sur l'interface WAN appropriée. Les routeurs sont des équipements de réseau actifs et intelligents, capables de participer à l'administration d'un réseau. Ils administrent les réseaux en exerçant un contrôle dynamique sur les ressources et en prenant en charge les tâches et les objectifs du réseau. Certains de ces objectifs sont la connectivité, des performances fiables, la supervision et la souplesse.

Ces liaisons de communication nécessitent des signaux au format approprié. Sur les lignes numériques, une unité CSU (*channel service unit*) et une unité DSU (*data service unit*) sont nécessaires. Ces deux unités sont souvent combinées en une seule, que l'on appelle CSU/DSU. L'unité CSU/DSU peut également être intégrée à la carte d'interface du routeur. 3


Une boucle numérique se termine au niveau d'une unité CSU/DSU.
Le routeur et l'unité CSU/DSU sont connectés par un câble série.

Un modem s'avère nécessaire si la boucle locale est analogique et non numérique. 4



Les modems transmettent des données sur les lignes téléphoniques vocales en modulant et en démodulant le signal. Les signaux numériques sont superposés sur un signal vocal analogique modulé en vue de sa transmission. Ce signal modulé se fait entendre sous la forme d'une série de sifflements lorsque vous activez le haut-parleur interne du modem. À la destination, les signaux analogiques sont reconvertis en signaux numériques, ou démodulés.

Lorsqu'un dispositif RNIS est utilisé comme liaison de communication, tout l'équipement relié au bus RNIS doit être compatible RNIS. La compatibilité est généralement intégrée à l'interface de l'ordinateur pour les connexions à accès commuté direct, ou à l'interface du routeur pour les connexions de LAN à WAN. Les équipements plus anciens, sans interface RNIS, nécessitent un adaptateur de terminal RNIS pour être compatibles.

Les serveurs de communication concentrent les communications entrantes des utilisateurs et les accès à distance à un réseau local. Ils peuvent comporter un mélange d'interfaces analogiques et numériques (RNIS) et prendre en charge des centaines d'utilisateurs simultanés.

Activité de média interactive

Mots croisés: Équipements et interfaces WAN

À la fin de cette activité, l'étudiant doit être capable de décrire les équipements et les interfaces associés aux connexions WAN.

2.1 Aperçu des technologies WAN

2.1.3 Normes WAN

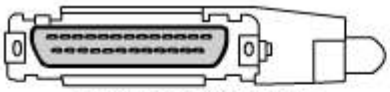
Les WAN utilisent le modèle de référence OSI, mais se concentrent principalement sur la couche 1 et la couche 2. Les normes WAN décrivent généralement les méthodes de livraison sur la couche physique et les caractéristiques requises pour la couche de liaison de données, notamment l'adressage physique, le contrôle de flux et l'encapsulation. Les normes WAN sont définies et gérées par plusieurs autorités reconnues. [1]

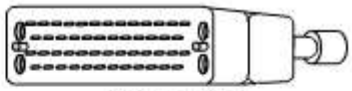
Acronyme	Organisation
ITU-T (was CCITT)	Union internationale des télécommunications - secteur de normalisation des télécommunications (UIT-T), anciennement Comité consultatif international télégraphique et téléphonique (CCITT)
ISO	Organisation internationale de normalisation
IETF	Groupe IETF
EIA	Electronic Industries Association
TIA	Telecommunications Industry Association

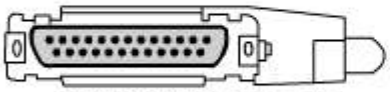
Les protocoles de couche physique décrivent comment fournir les connexions électriques, mécaniques, opérationnelles et fonctionnelles aux services fournis par un fournisseur d'accès. Certaines des normes liées à la couche physique commune sont énumérées à la figure 2 et leurs connecteurs illustrés à la figure 3

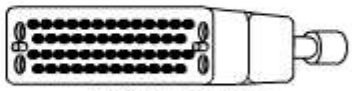
Norme	Description
EIA/TIA-232	Autorise des débits jusqu'à 64 kbits/s sur un connecteur D 25 broches sur de courtes distances. Anciennement désigné par RS-232. La spécification ITU-T V.24 est effectivement identique.
EIA/TIA-449/530	Version plus rapide (pouvant atteindre 2 Mbits/s) de la norme EIA/TIA-232. Elle utilise un connecteur D de 36 broches et est capable de prendre en charge des câbles plus longs. Il en existe plusieurs versions. Également appelée RS-422 et RS-423.
EIA/TIA-612/613	L'interface HSSI (High Speed Serial Interface), qui offre un accès aux services à des vitesses atteignant 52 Mbits/s sur un connecteur D à 60 broches.
V.35	Norme de l'ITU-T relative aux communications synchrones entre un équipement d'accès réseau et un réseau de transmission de paquets à des débits pouvant atteindre 48 kbits/s. Elle s'appuie sur un connecteur rectangulaire à 34 broches.
X.21	Norme de l'ITU-T relative aux communications numériques synchrones. Elle s'appuie sur un connecteur à 15 broches.

.

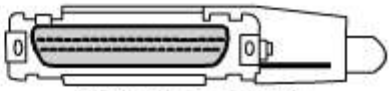

EIA/TIA-232 Mâle

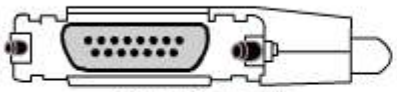

V.35 Mâle

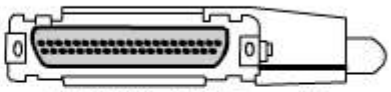

EIA/TIA-232 Femelle

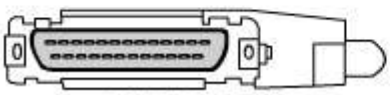

V.35 Femelle

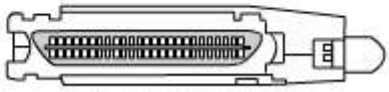
X.21 Mâle


EIA/TIA-449 Mâle

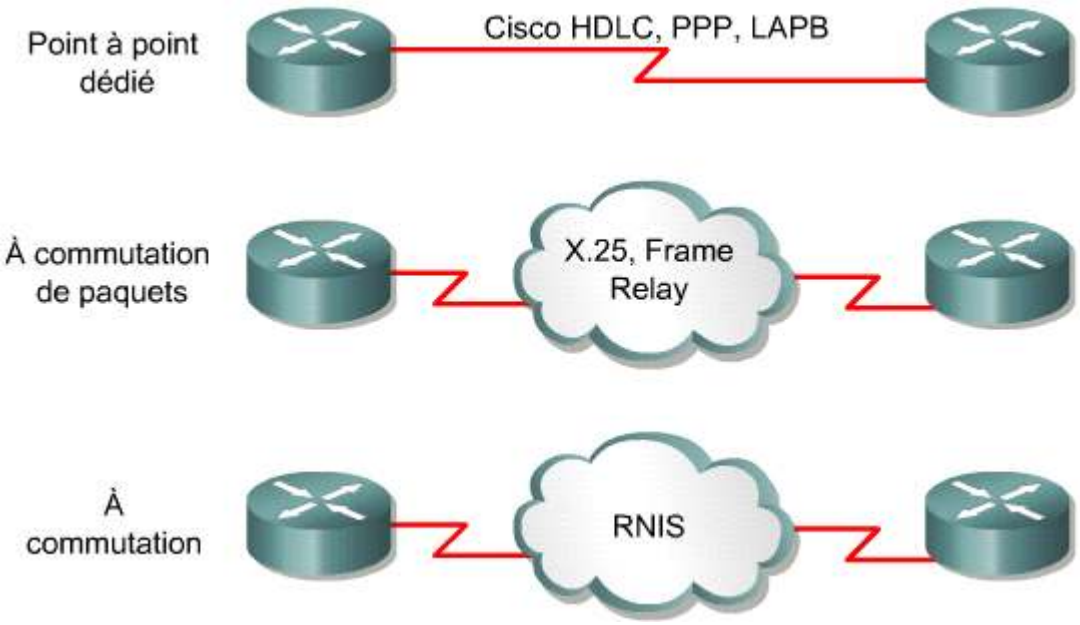

X.21 Femelle


EIA/TIA-449 Femelle


EIA-530 Mâle


EIA-613 HSSI Mâle

Les protocoles de la couche de liaison de données définissent la manière dont les données sont encapsulées en vue de leur transmission vers des sites distants, ainsi que les mécanismes de transfert des trames obtenues. Différentes technologies sont utilisées, notamment RNIS, Frame Relay, ou le mode de transfert asynchrone ATM (*Asynchronous Transfer Mode*). Ces protocoles utilisent tous le même mécanisme de tramage de base, HDLC (*high-level data link control*), une norme ISO ou l'un de ses sous-ensembles ou variantes. [4]



Activité de média interactive

Mots croisés: Normes WAN

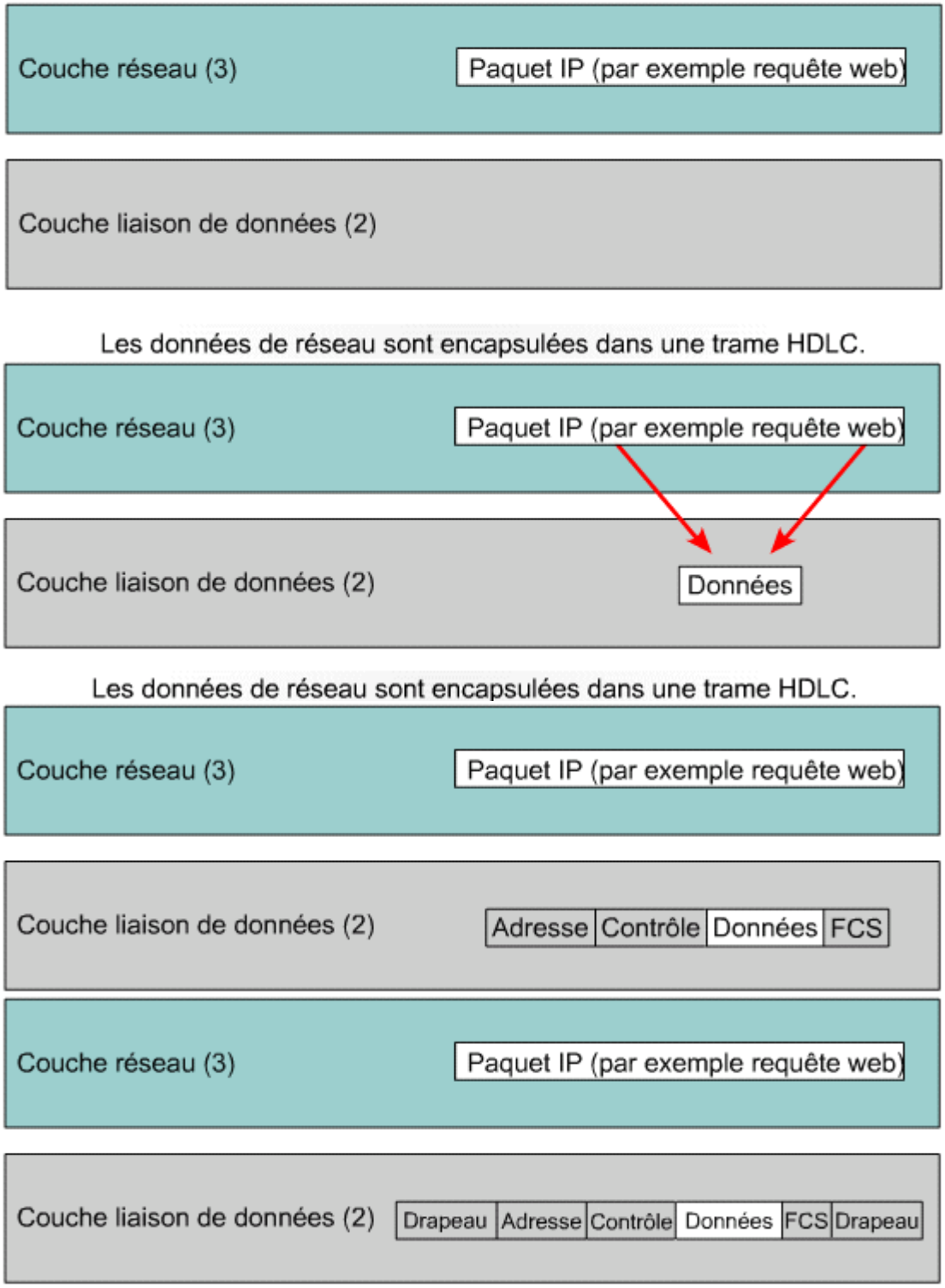
À la fin de cette activité, l'étudiant sera en mesure d'identifier les diverses normes WAN.

2.1 Aperçu des technologies WAN

2.1.4 Encapsulation WAN

Les données de la couche réseau sont transférées à la couche de liaison de données en vue de leur livraison sur une liaison physique, généralement point-à-point sur une connexion WAN. La couche de liaison de données établit une trame autour des données de la couche réseau, de telle sorte que les vérifications et contrôles nécessaires puissent être appliqués. Chaque type de connexion WAN utilise un protocole de couche 2 pour encapsuler le trafic pendant qu'il traverse la liaison longue distance. Pour assurer que le bon protocole d'encapsulation est utilisé, le type d'encapsulation de couche 2 utilisé pour l'interface série de chaque routeur doit être configuré. Le choix du protocole d'encapsulation est fonction de la technologie WAN et de l'équipement. Le tramage s'appuie essentiellement sur la norme HDLC.

Le tramage HDLC offre une livraison fiable des données sur des lignes qui ne sont pas fiables et inclut des mécanismes de contrôle de flux et d'erreur. [1]



La trame commence et se termine toujours par un champ indicateur sur 8 bits, selon le motif 01111110. Comme ce motif est susceptible de survenir dans les données mêmes, le système HDLC émetteur insère toujours un bit 0 tous les cinq 1 du champ de données, de telle sorte qu'en pratique, la séquence de l'indicateur peut seulement survenir aux extrémités de la trame. Le système récepteur supprime les bits insérés. Quand les trames sont transmises de façon consécutive, l'indicateur de fin de la première trame sert d'indicateur de début de la suivante.

Le champ adresse n'est pas requis pour les liaisons WAN, qui sont presque toujours point-à-point. Le champ adresse est toujours présent et peut avoir une longueur d'un ou deux octets. Le champ de contrôle indique le type de trame, qui peut être de type information, supervision ou non numéroté:

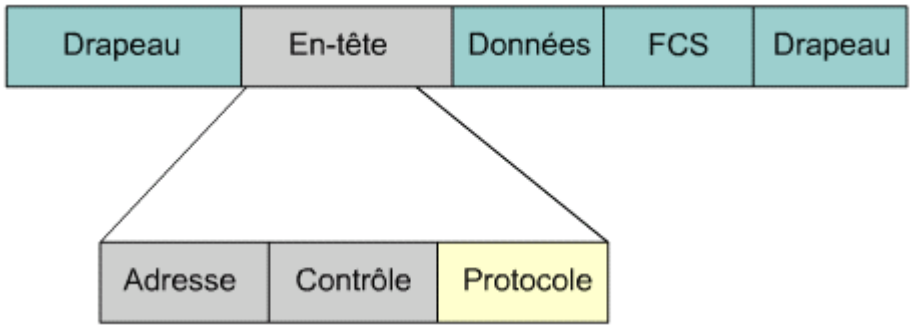
- Les trames non-numérotées transportent des messages de configuration de ligne.
- Les trames d'informations transportent les données de couche de réseau.
- Les trames de supervision contrôlent le flux de trames d'informations et demandent la retransmission des données en cas d'erreur.

Le champ de contrôle fait généralement un octet, mais sera de deux octets pour les systèmes à fenêtres glissantes. Combinés, les champs d'adresse et de contrôle sont appelés l'en-tête de trame. Les données encapsulées suivent le champ de contrôle. Une séquence de vérification de trame (FCS) utilise le mécanisme de code de redondance cyclique (CRC) pour établir un champ de deux ou quatre octets.

Plusieurs protocoles de liaison de données sont utilisés, notamment des sous-ensembles et des versions propriétaires de HDLC. 2

Protocole	Utilisation
Procédure d'accès en mode équilibré LAPB	X.25
Protocole de liaison LAPD	RNIS canal D
Procédure de liaison LAPF	Frame Relay
HDLC (High Level Data Link Control)	Valeur Cisco par défaut
PPP (protocole point à point)	Connexions séries WAN commutées

PPP et la version Cisco de HDLC disposent d'un champ supplémentaire dans l'en-tête afin d'identifier le protocole de couche réseau des données encapsulées. 3

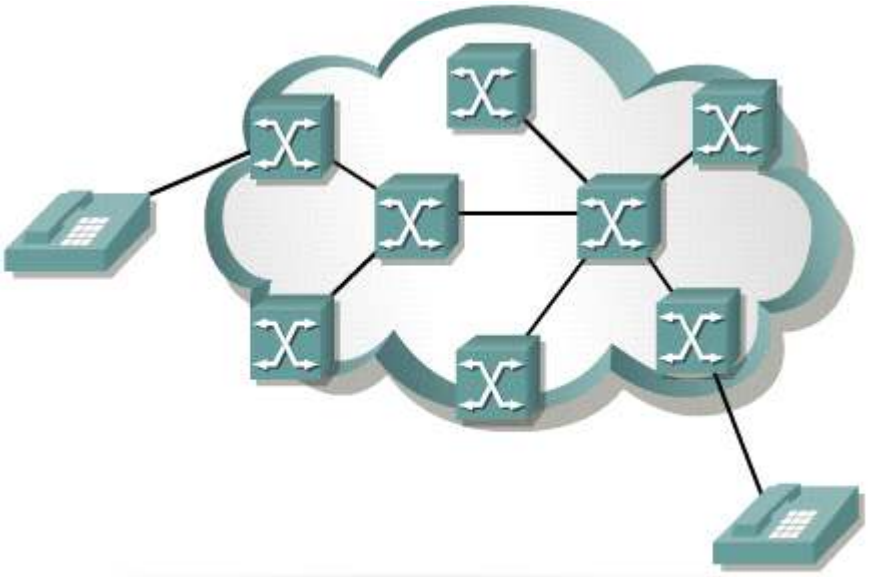


2.1 Aperçu des technologies WAN

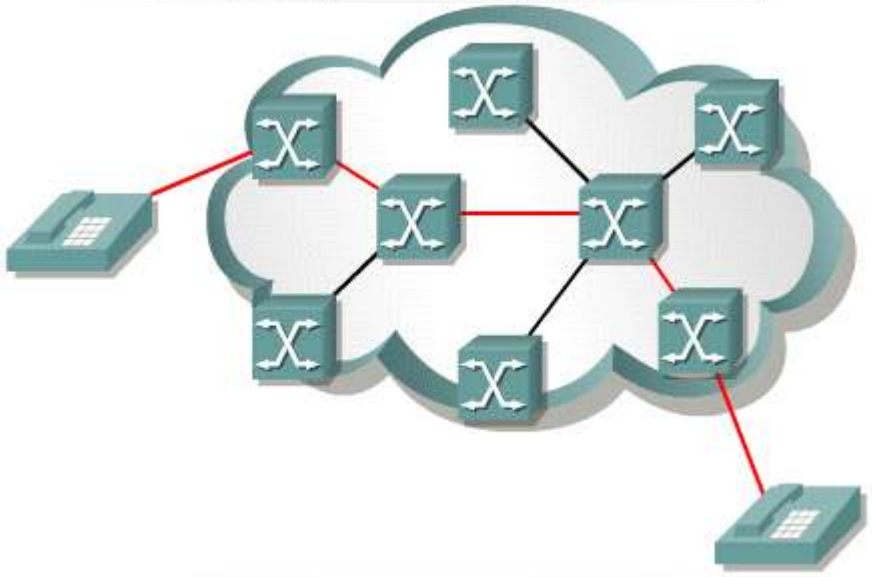
2.1.5 Commutation de paquets et de circuits

Les réseaux à commutation de paquets ont été développés pour éviter les dépenses entraînées par les réseaux à commutation de circuits publics et pour offrir une technologie WAN plus économique.

Lorsqu'un abonné passe un appel téléphonique, le numéro appelé sert à définir des commutations dans les échanges effectués sur la route de l'appel, de telle sorte qu'il existe un circuit continu entre l'appelant et l'appelé. Du fait de l'opération de commutation utilisée pour établir le circuit, le système téléphonique adopte le nom de réseau à commutation de circuits. Si les téléphones sont remplacés par des modems, le circuit commuté peut également transporter des données informatiques. 1



La numérotation configure un circuit physique sur le système.

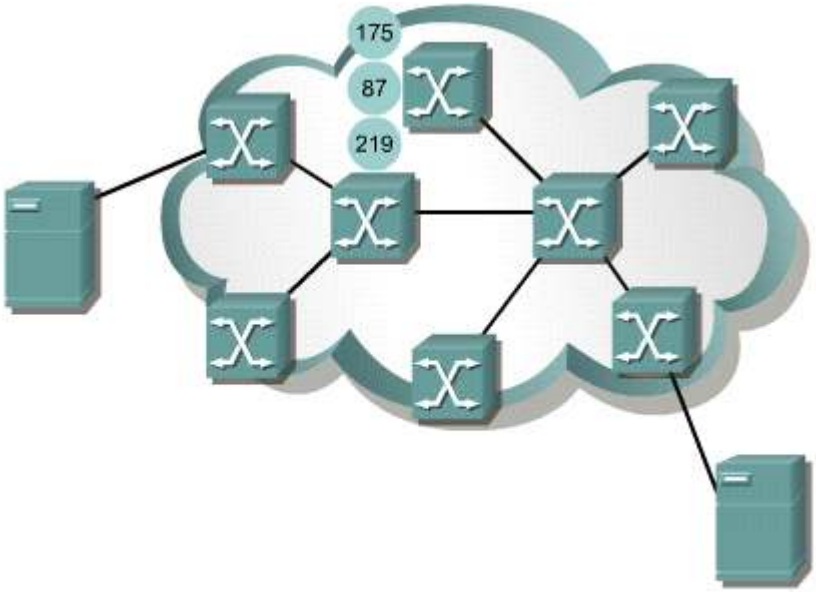


La numérotation configure un circuit physique sur le système.

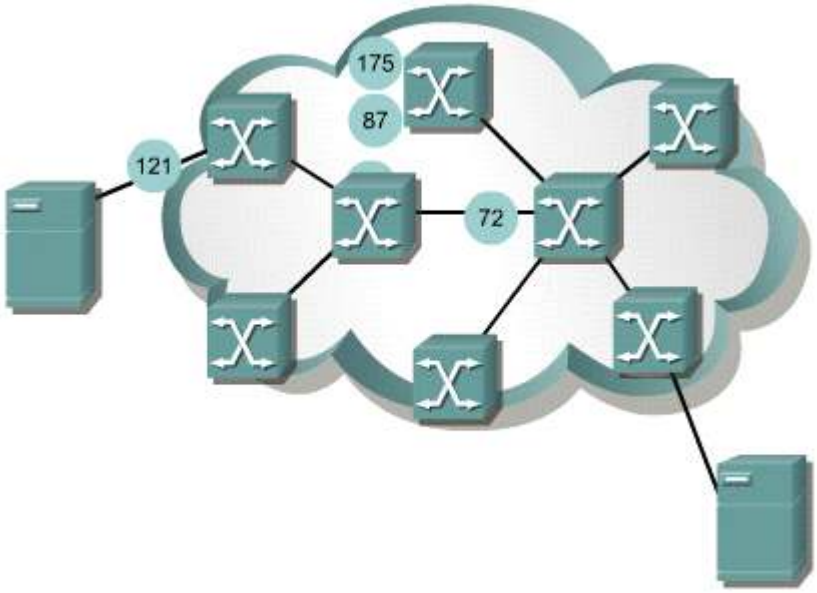
Le chemin interne emprunté par le circuit entre les échanges est partagé par un certain nombre de conversations. Le multiplexage temporel (TDM - *Time division multiplexing*) permet de partager la connexion à tour de rôle entre chaque conversation. Le TDM assure qu'une connexion de capacité fixe soit mise à la disposition de l'abonné.

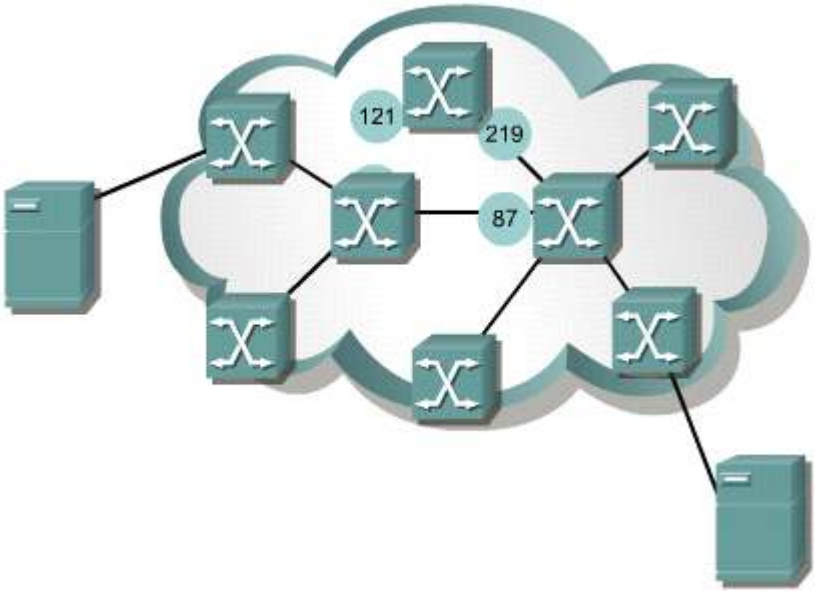
Si le circuit transporte des données informatiques, l'utilisation de cette capacité fixe risque de ne pas être efficace. Par exemple, si le circuit sert à accéder à Internet, une poussée d'activité s'effectue sur les circuits pendant le transfert d'une page Web. Elle peut être suivie par aucune activité pendant que l'utilisateur lit la page, puis une autre poussée d'activité pendant que la page suivante est transférée. Cette variation d'utilisation entre aucune et maximum est typique du trafic réseau informatique. Comme l'abonné a l'utilisation exclusive de son allocation de capacité fixe, les circuits commutés constituent généralement une méthode coûteuse de déplacement des données.

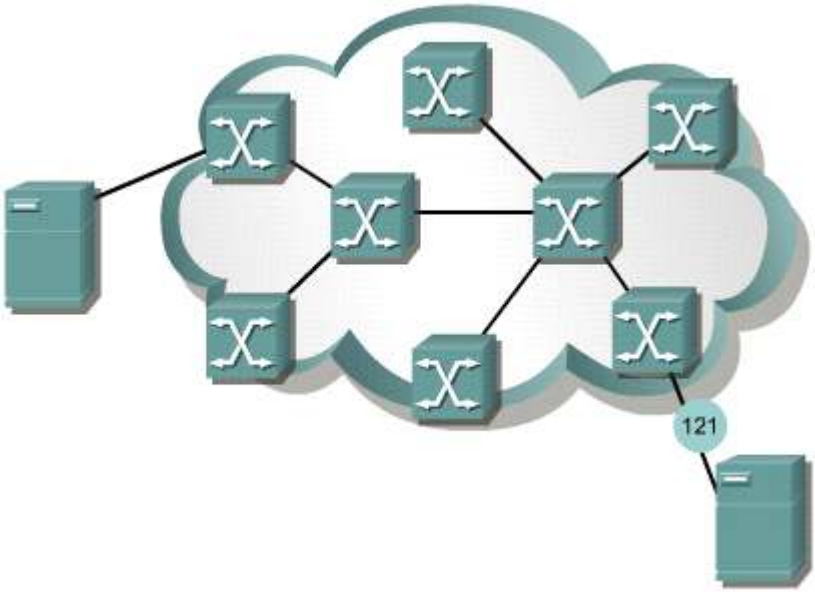
Une autre possibilité consiste à seulement allouer la capacité au trafic quand celui-ci s'avère nécessaire et partager la capacité disponible entre de nombreux utilisateurs. Avec une connexion à commutation de circuits, les bits de données placés sur le circuit sont automatiquement remis à l'extrémité distante, car le circuit est déjà établi. Si le circuit doit être partagé, un mécanisme doit identifier les bits, de manière à ce que le système sache où les remettre. Il est difficile d'étiqueter des bits individuels et ceux-ci sont donc rassemblés dans des groupes appelés cellules, trames ou paquets. Le paquet passe d'un échange à l'autre pour être remis par l'intermédiaire du réseau du fournisseur d'accès. On désigne les réseaux qui mettent en oeuvre ce système par le nom de réseaux à commutation de paquets. 2



Les données libellées sont transférées d'un commutateur à l'autre.
Il se peut qu'elles doivent attendre leur tour sur une liaison.







Les liaisons qui connectent les commutateurs du réseau du fournisseur d'accès appartiennent à un abonné en particulier au cours du transfert des données, ce qui permet à de nombreux abonnés de partager la liaison. Les coûts peuvent être considérablement moins élevés que ceux d'une connexion dédiée à commutation de circuits. Les données des réseaux à commutation de paquets sont soumises à des retards imprévisibles lorsque des paquets individuels attendent que les paquets d'autres abonnés soient transmis par un commutateur.

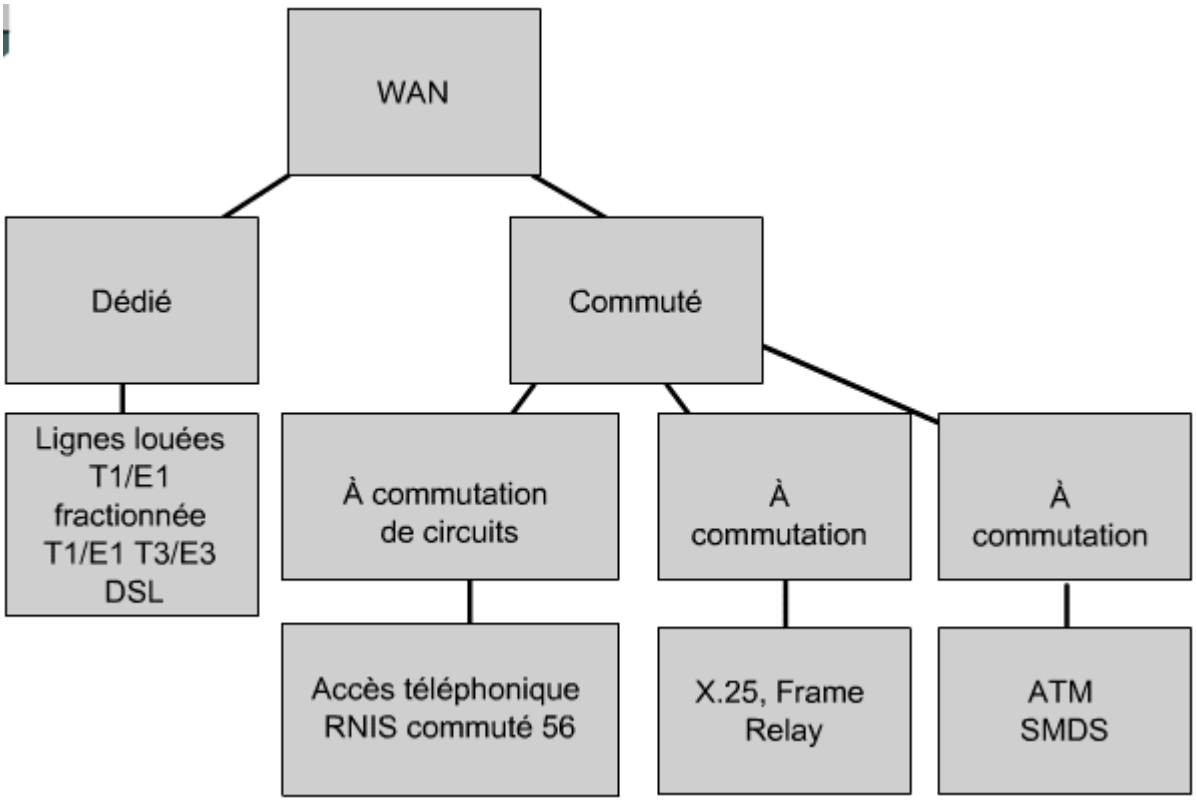
À partir des informations d'adresse fournies dans chaque paquet, les commutateurs d'un réseau à commutation de paquets déterminent le lien vers lequel le paquet doit ensuite être envoyé. Il existe deux approches à cette détermination des liaisons ; non-orienté connexion et orienté connexion. Les systèmes non-orientés connexion, tels qu'Internet, transportent des données d'adressage complètes dans chaque paquet. Chaque commutateur doit évaluer l'adresse pour déterminer où envoyer le paquet. Les systèmes orientés connexion prédéterminent la route de chaque paquet, qui n'a alors besoin que d'un identificateur. Dans le cas de Frame Relay, il s'agit des identificateurs de contrôle de liaison de données (DLCI). Le commutateur détermine la route à suivre en recherchant l'identificateur dans des tables en mémoire. Le jeu d'entrées des tables identifie un itinéraire ou circuit particulier sur le système. Si ce circuit n'existe physiquement que lorsqu'un paquet se déplace dessus, il prend le nom de circuit virtuel (VC – *Virtual Circuit*).

Les entrées qui constituent un circuit virtuel peuvent être établies par une requête de connexion envoyée sur le réseau. Dans ce cas, le circuit obtenu est appelé circuit virtuel commuté (SVC). Les données qui sont transportées sur des circuits virtuels commutés doivent attendre que les entrées de la table aient été configurées. Une fois établi, le circuit virtuel commuté peut rester actif pendant des heures, des jours ou des semaines. Quand il est nécessaire qu'un circuit reste disponible en permanence, un circuit virtuel permanent (PVC) est établi. Les entrées de la table sont chargées par les commutateurs au démarrage, de telle sorte que le circuit virtuel permanent soit toujours disponible.

2.1 Aperçu des technologies WAN

2.1.6 Options de liaison WAN

La figure 1 fournit une vue d'ensemble des options de liaison WAN.



La commutation de circuits établit une connexion physique dédiée pour la voix ou les données entre un expéditeur et un destinataire. Avant que la communication ne commence, il est nécessaire d'établir la connexion en configurant les commutateurs. Ceci est effectué par le système téléphonique, au moyen du numéro composé. Le protocole RNIS s'utilise sur des lignes numériques ou vocales.

Pour éviter les retards associés à la configuration d'une connexion, les opérateurs téléphoniques proposent également des circuits permanents. Ces lignes dédiées ou concédées offrent un débit plus élevé que celui d'un circuit commuté. Les connexions à commutation de circuits peuvent, par exemple, être:

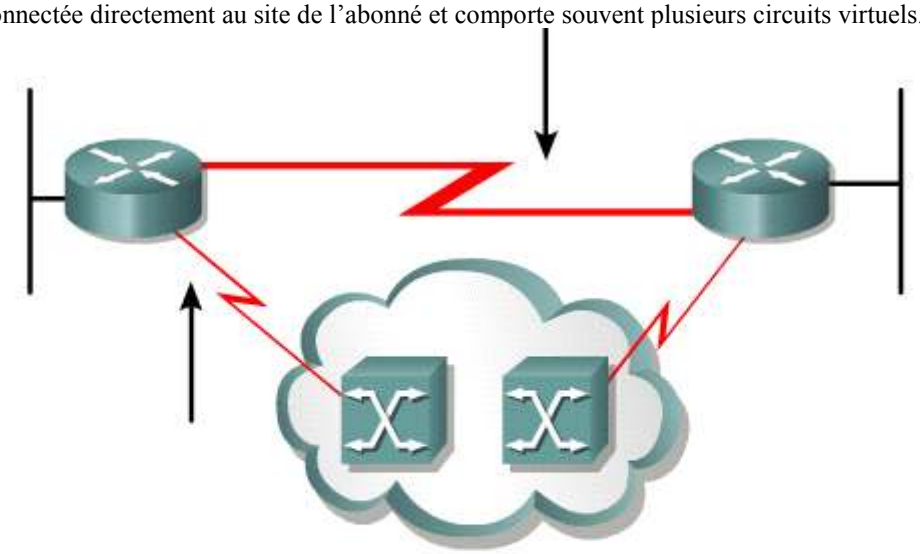
- Le réseau téléphonique analogique
- Le RNIS BRI (accès de base)
- Le RNIS PRI (accès primaire)

De nombreux utilisateurs de WAN n'utilisent pas de façon optimale la bande passante fixe à leur disposition avec des circuits dédiés, commutés ou permanents, car le flux de données fluctue. Les fournisseurs d'accès disposent de réseaux de données permettant de desservir ces utilisateurs de façon plus appropriée. Dans ces réseaux, les données sont transmises dans des cellules, des trames ou des paquets libellés, par l'intermédiaire d'un réseau à commutation de paquets. Comme les liaisons internes entre les commutateurs sont partagées entre plusieurs utilisateurs, les coûts de la commutation de paquets sont inférieurs à ceux de la commutation de circuits. Les délais (latence) et la variabilité des délais (gigue) sont plus importants dans la commutation de paquets que sur les réseaux à commutation de circuits. En effet, comme les liaisons sont partagées, l'intégralité des paquets doit avoir été reçue par un commutateur avant de passer au suivant. Malgré la latence et la gigue inhérentes aux réseaux partagés, la technologie moderne autorise un transport satisfaisant des communications vocales, voire vidéo, sur ces réseaux.

Les réseaux à commutation de paquets peuvent établir des routes via les commutateurs pour des connexions de bout en bout en particulier. Les routes établies au démarrage des commutateurs sont des circuits virtuels permanents. Les routes établies à la demande sont des SVC. Si le routage n'est pas préétabli, mais déterminé par chaque commutateur pour chaque paquet, le réseau est désigné par le terme «non-orienté connexion».

Pour se connecter à un réseau à commutation de paquets, un abonné nécessite une boucle locale jusqu'à l'emplacement le plus proche auquel le fournisseur d'accès met le service à disposition. C'est ce que l'on appelle le point de présence (POP – *point-of-presence*) du service. Il s'agit généralement d'une ligne dédiée concédée. Elle est bien plus courte qu'une ligne concédée

connectée directement au site de l'abonné et comporte souvent plusieurs circuits virtuels. 2



Les réseaux locaux peuvent être connectés par une longue ligne louée ou par des lignes louées plus courtes raccordées à un réseau à commutation de paquets. Ce dernier sera responsable pour le transport sur des longues distances.

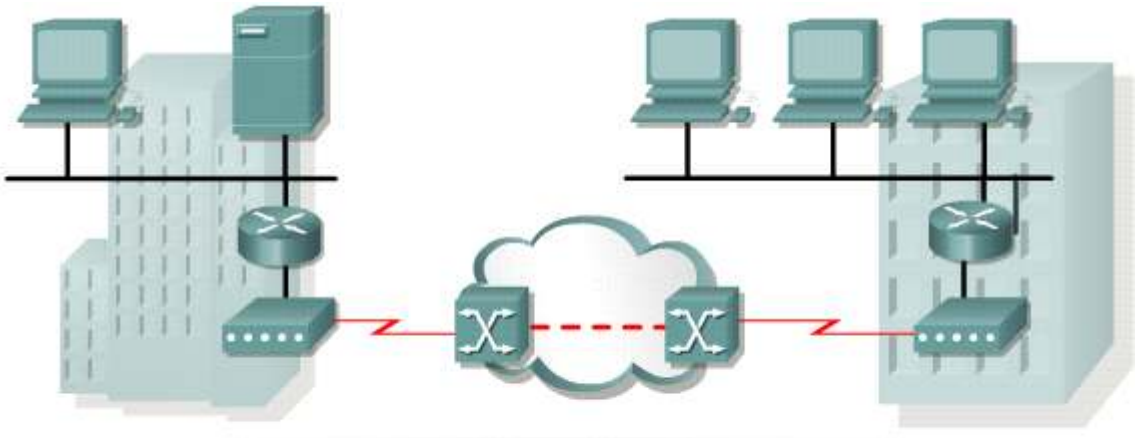
Comme il est probable que tous les circuits virtuels n'aient pas besoin d'une demande maximale simultanément, la capacité de la ligne concédée peut être inférieure à la somme des circuits virtuels individuels. Des exemples de connexions à commutation de paquets ou de cellules sont fournis ci-dessous:

- Frame Relay
- X.25
- ATM

2.2 Technologies WAN

2.2.1 Connexions commutées analogiques

Lorsque des transferts de données intermittents de faible volume sont nécessaires, les modems et les lignes téléphoniques commutées analogiques fournissent des connexions commutées de faible capacité et dédiées. 1



Réseau WAN construit avec des connexions intermittentes au moyen d'un modem et du réseau téléphonique vocal.

La téléphonie traditionnelle utilise un câble de cuivre, appelé la boucle locale, pour connecter le combiné téléphonique situé dans les locaux de l'abonné au réseau téléphonique commuté public (RTCP). Le signal de la boucle locale pendant une communication est un signal électronique variant continuellement et qui constitue une traduction de la voix de l'abonné.

La boucle locale n'est pas adaptée au transport direct de données informatiques binaires, mais un modem permet d'envoyer des données informatiques par le réseau téléphonique vocal. Le modem module les données binaires en un signal analogique à la source et démodule ce signal en données binaires une fois arrivé à destination.

Les caractéristiques physiques de la boucle locale et sa connexion au RTCP limitent le débit de ce signal. La limite supérieure se situe aux environs de 33 Kbits/s. Le débit peut être augmenté à environ 56 Kbits/s si le signal passe directement par une connexion numérique.

Pour les PME, cela peut s'avérer adéquat pour l'échange de chiffres de vente, de prix, de rapports de routine et de courrier électronique. En utilisant la numérotation automatique la nuit ou le week-end pour le transfert de gros fichiers et la sauvegarde de données, vous pouvez bénéficier de tarifs heures creuses plus intéressants. Les tarifs sont fondés sur la distance entre les points d'extrémité, l'heure du jour et la durée de l'appel.

Les avantages du modem et des lignes analogiques sont la simplicité, la disponibilité et le faible coût de mise en oeuvre. Les inconvénients en sont les faibles débits et un temps de connexion relativement long. Le circuit dédié fourni par la connexion commutée présente peu de délai ou de gigue pour le trafic point-à-point, mais le trafic vocal ou vidéo ne fonctionne pas de façon adéquate à des débits relativement faibles.

Activité de média interactive

Case à cocher: Technologies WAN – Accès commuté analogique

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées à un circuit commuté analogique.

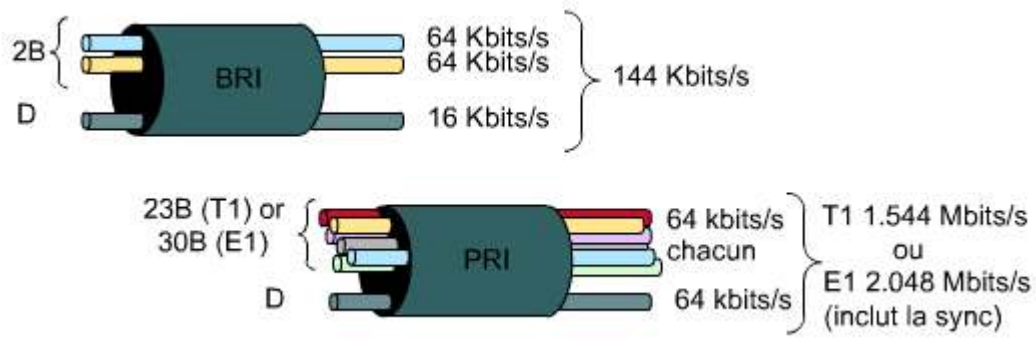
2.2 Technologies WAN

2.2.2 RNIS

Les connexions internes, ou agrégations, du RTCP sont passées des signaux analogiques de multiplexage à division fréquentielle aux signaux numériques de multiplexage temporel (TDM – *Time Division Multiplexed*). L'étape suivante consiste évidemment à permettre à la boucle locale de transporter des signaux numériques offrant des connexions commutées de plus haute capacité.

Le réseau RNIS transforme la boucle locale en une connexion numérique TDM. La connexion utilise des canaux Bearer à 64 kbits/s (B) pour transporter la voix ou les données et un canal delta de signal (D) destiné à la configuration de la communication et à d'autres fonctions.

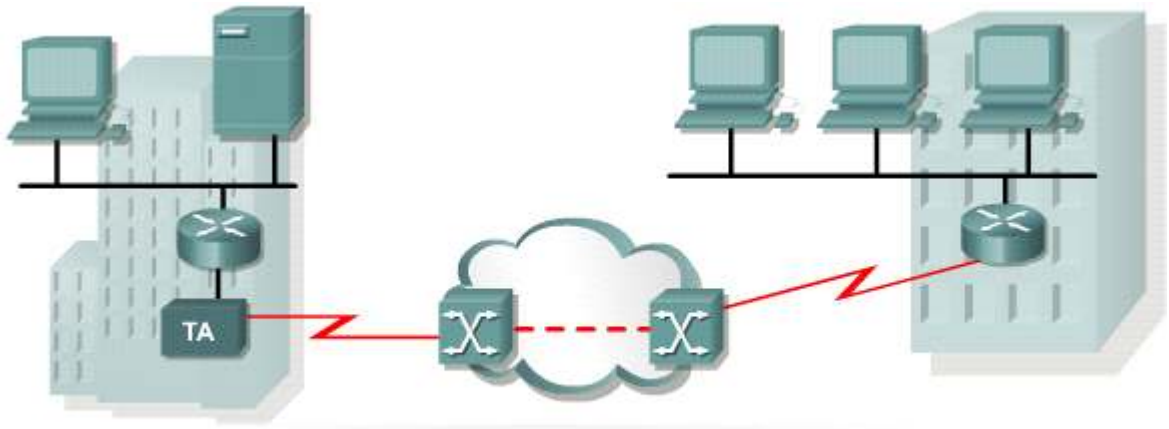
Le réseau RNIS BRI accès de base est destiné aux utilisateurs individuels et aux petites entreprises et offre deux canaux B à 64 kbits/s et un canal D à 16 kbits/s. Pour les installations de plus grande taille, il existe une version de RNIS PRI accès primaire. L'accès PRI offre vingt trois canaux B et à 64 kbits/s et un canal D à 64 kbits/s en Amérique du Nord, pour un débit total de 1 544 Mbits/s. Ceci inclut une surcharge pour la synchronisation. En Europe, en Australie et dans d'autres régions du monde, RNIS PRI offre trente canaux B et un canal D, pour un débit total allant jusqu'à 2 048 Mbits/s, surcharge de synchronisation comprise. [1]



En Amérique du Nord, PRI correspond à une connexion T1. Le débit du PRI international correspond à une connexion E1.

Le canal D du BRI est sous-utilisé, car il n'a que deux canaux B à gérer. Certains fournisseurs laissent le canal D transporter des données à bas débit, telles que les connexions X.25 à 9.6 kbits/s.

Pour les petits réseaux WAN, le RNIS BRI peut offrir un mécanisme de connexion idéal. La durée de mise en fonction du BRI est inférieure à une seconde et son canal B à 64 kbits/s offre une capacité plus importante que celle d'une liaison par modem analogique. 2



Les routeurs peuvent comporter des interfaces RNIS ou se connecter à un adaptateur de terminal.

Si une capacité plus importante est nécessaire, il est possible d'activer un deuxième canal B, pour un total de 128 kbits/s. Bien qu'inadéquat pour la vidéo, ceci autorise plusieurs conversations vocales simultanées et plus du trafic de données.

Une autre application courante du RNIS consiste à fournir des capacités supplémentaires en fonction des besoins à une connexion par ligne louée. La ligne louée est dimensionnée pour transporter des charges de trafic moyenne et le RNIS vient s'y ajouter lors des périodes de pointe. Le RNIS sert également de ligne de secours en cas de défaillance de la ligne louée. Les tarifs RNIS sont calculés par canal B et sont similaires à ceux des connexions analogiques vocales.

Avec RNIS PRI, plusieurs canaux B peuvent être connectés entre deux points d'extrémité. Cela rend possible les vidéoconférences et les connexions de données haut débit sans latence ni gigue. Plusieurs connexions peuvent finir par s'avérer très coûteuses sur de longues distances.

Activité de média interactive

Case à cocher: Technologies WAN – Accès commuté RNIS

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées à un circuit commuté RNIS.

2.2 Technologies WAN

2.2.3 Ligne louée

Lorsque des connexions dédiées permanentes sont nécessaires, des lignes louées, dont le débit peut s'élever à 2,5 Gbits/s sont utilisées.

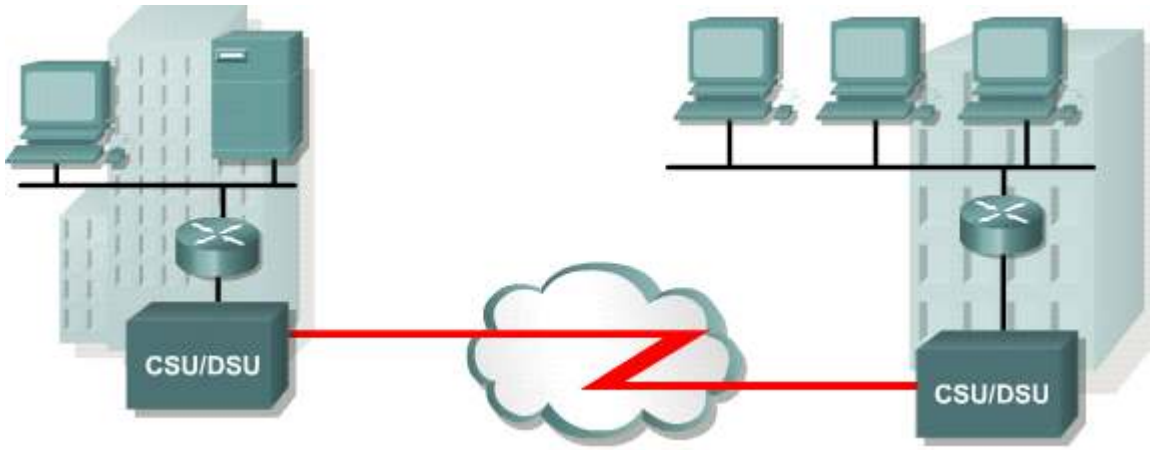
Une liaison point-à-point fournit un chemin de communication WAN préétabli entre les locaux du client et une destination distante par l'intermédiaire du réseau du fournisseur d'accès. Les lignes point-à-point sont généralement louées à un opérateur et prennent le nom de lignes louées. Il existe différentes capacités de lignes louées. 1

Type de ligne	Norme de signal	Débit binaire
56	DS0	56 Kbits/s
64	DS0	64 Kbits/s
T1	DS1	1.544 Mbits/s
E1	ZM	2.048 Mbits/s
E3	M3	34.064 Mbits/s
J1	Y1	2.048 Mbits/s
T3	DS3	44.736 Mbits/s
OC-1	SONET	51.84 Mbits/s
OC-3	SONET	155.54 Mbits/s
OC-9	SONET	466.56 Mbits/s
OC-12	SONET	622.08 Mbits/s
OC-18	SONET	933.12 Mbits/s
OC-24	SONET	1244.16 Mbits/s
OC-36	SONET	1866.24 Mbits/s
OC-48	SONET	2488.32 Mbits/s

Le prix de ces circuits dédiés est généralement fondé sur le débit, ainsi que sur la distance entre les deux points connectés. Les liaisons point-à-point sont généralement plus coûteuses que les services partagés tels que Frame Relay. Le coût des liaisons louées peut être important lorsqu'elles servent à connecter plusieurs sites. Toutefois, le coût de la ligne louée est parfois compensé par les avantages qu'elle offre. L'aspect dédié de la ligne permet d'éviter la latence ou la gigue entre les points d'extrémité. Une disponibilité constante est essentielle à certaines applications, telles que le commerce électronique.

Le port série d'un routeur est requis pour chaque connexion sur ligne louée. Une unité CSU/DSU et le circuit provenant du fournisseur d'accès sont également requis.

Les lignes louées sont utilisées extensivement pour construire des WAN et offrent une connexion dédiée permanente. 2



Elles constituent traditionnellement le meilleur choix de connexion, mais présentent plusieurs inconvénients. Le trafic des WAN est souvent variable et les lignes louées offrent une capacité fixe. En conséquence, il est rare que la bande passante de la ligne réponde exactement aux besoins. Par ailleurs, chaque point d'extrémité nécessite une interface sur le routeur, ce qui entraîne une augmentation des coûts en équipement. Toute modification de la ligne louée nécessite généralement une intervention sur le site par l'opérateur, en vue de modifier la capacité.

Les lignes louées fournissent des connexions point-à-point directes entre les réseaux locaux d'entreprise et connectent les filiales individuelles à un réseau à commutation de paquets. Plusieurs connexions peuvent être multiplexées sur une ligne louée, de façon à fournir des liaisons plus courtes et un nombre moins important d'interfaces requises.

Activité de média interactive

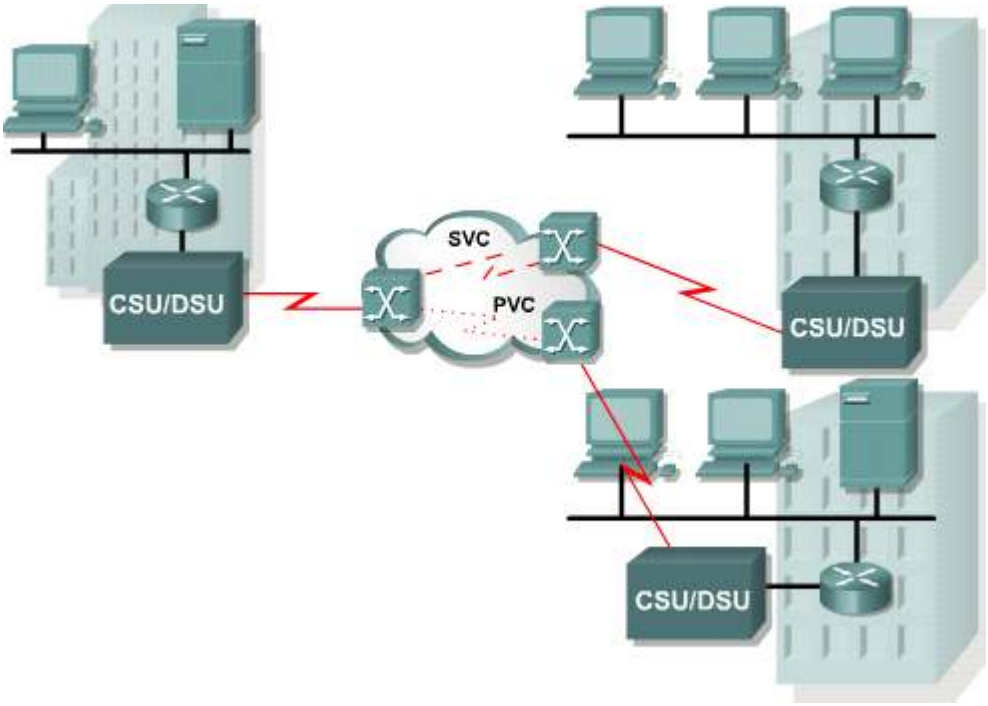
Case à cocher: Technologies WAN – Lignes louées

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées à une connexion par ligne louée.

2.2 Technologies WAN

2.2.4 X.25

En réaction aux coûts des lignes louées, les fournisseurs d'accès ont introduit des réseaux à commutation de paquets sur des lignes partagées, en vue de réduire les coûts. Le premier de ces réseaux à commutation de paquets a été normalisé sous le groupe de protocoles X.25. X.25 fournit une capacité variable de faible débit, qui peut être commutée ou permanente. 1



X.25 est un protocole de couche de réseau avec lequel les abonnés reçoivent une adresse réseau. Des circuits virtuels peuvent être établis sur le réseau, avec des paquets de requête d'appel vers l'adresse de destination. Le circuit virtuel commuté obtenu est identifié par un numéro de canal. Des paquets de données identifiés par le numéro de canal sont remis à l'adresse correspondante. Plusieurs canaux peuvent être actifs sur une seule connexion.

Les abonnés se connectent au réseau X.25 au moyen de lignes louées ou de connexions commutées. Les réseaux X.25 peuvent également établir des canaux prédéfinis entre les abonnés, afin de fournir un circuit virtuel permanent.

X.25 peut s'avérer très économique, car les tarifs sont fondés sur la quantité de données remises, et non sur la durée ou la distance de connexion. Les données peuvent être remises à n'importe quel débit, dans les limites de la capacité de la connexion. Ceci procure une certaine souplesse. Les réseaux X.25 offrent généralement un débit faible, à un maximum de 48 kbits/s. Par ailleurs, les paquets de données sont soumis aux délais typiques des réseaux partagés.

La technologie X.25 n'est plus aussi diffusée aux États-Unis qu'auparavant en tant que technologie WAN. En effet, les réseaux Frame Relay ont remplacé le X.25 chez de nombreux fournisseurs.

Parmi les applications X.25 typiques, on trouve les lecteurs de carte sur point de vente. Ces lecteurs utilisent X.25 en mode commuté pour valider les transactions sur un ordinateur central. Certaines entreprises font également appel à des réseaux X.25 à valeur ajoutée pour transférer des factures EDI (*Electronic Data Interchange*), des notes de chargement et d'autres documents commerciaux. Pour ces applications, le bas débit et la latence élevée ne constituent pas une préoccupation, car son coût peu élevé rend le X.25 très économique.

Activité de média interactive

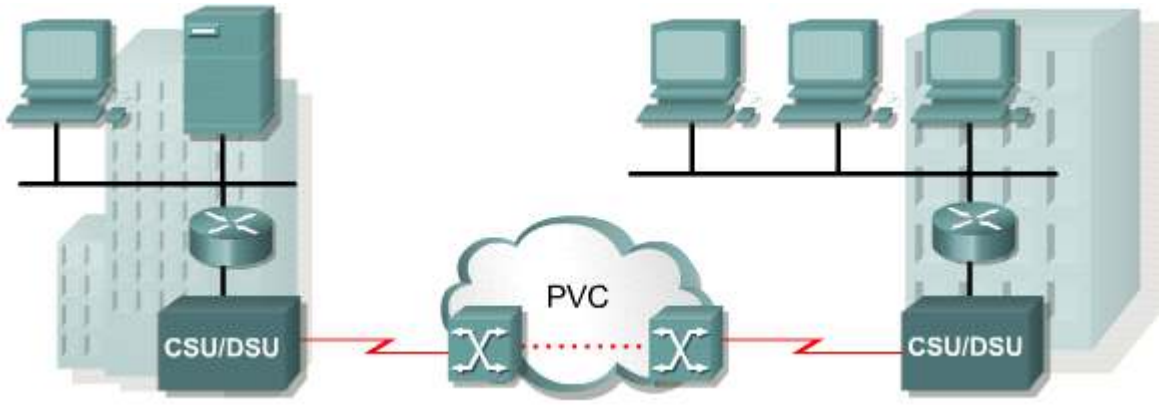
Case à cocher: Technologies WAN X.25

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées à une connexion X.25.

2.2 Technologies WAN

2.2.5 Frame Relay

Avec l'augmentation de la demande d'une commutation de paquets au débit plus élevé et à la latence moins importante, les fournisseurs d'accès ont introduit les réseaux Frame Relay. Bien que la configuration réseau semble similaire à celle de la technologie X.25, les débits peuvent couramment atteindre 4 Mbits/s, certains fournisseurs proposant même des débits plus élevés. 1



Plusieurs aspects différencient les technologies Frame Relay et X.25. Avant tout, il s'agit d'un protocole bien plus simple, qui fonctionne au niveau de la couche de liaison de données au lieu de la couche réseau.

Frame Relay ne met en oeuvre aucun contrôle d'erreur ou de flux. La gestion simplifiée des trames entraîne une réduction de la latence et des mesures prises pour éviter l'accumulation des trames sur les commutateurs intermédiaires permettent de réduire les phénomènes de gigue.

La plupart des connexions Frame Relay sont des circuits virtuels permanents et non des circuits virtuels commutés. La connexion à la périphérie du réseau s'effectue souvent sur une ligne louée, mais des connexions commutées sont disponibles auprès de certains fournisseurs utilisant des lignes RNIS. Le canal RNIS D sert à configurer un circuit virtuel commuté sur un ou plusieurs canaux B. Les tarifs Frame Relay sont fondés sur la capacité du port de connexion, à la périphérie du réseau. Les facteurs supplémentaires sont la capacité convenue et le débit de données garanti des divers circuits virtuels permanents passant par le port.

Le Frame Relay fournit un débit partagé moyen pouvant transporter du trafic vocal et de données. La technologie Frame Relay s'avère idéale pour connecter les réseaux locaux d'entreprise. Le routeur du réseau local ne nécessite qu'une interface, même avec plusieurs circuits virtuels. La courte ligne louée vers la périphérie du réseau Frame Relay autorise des connexions économiques entre des réseaux locaux largement dispersés.

Activité de média interactive

Case à cocher: Technologies WAN – Frame Relay

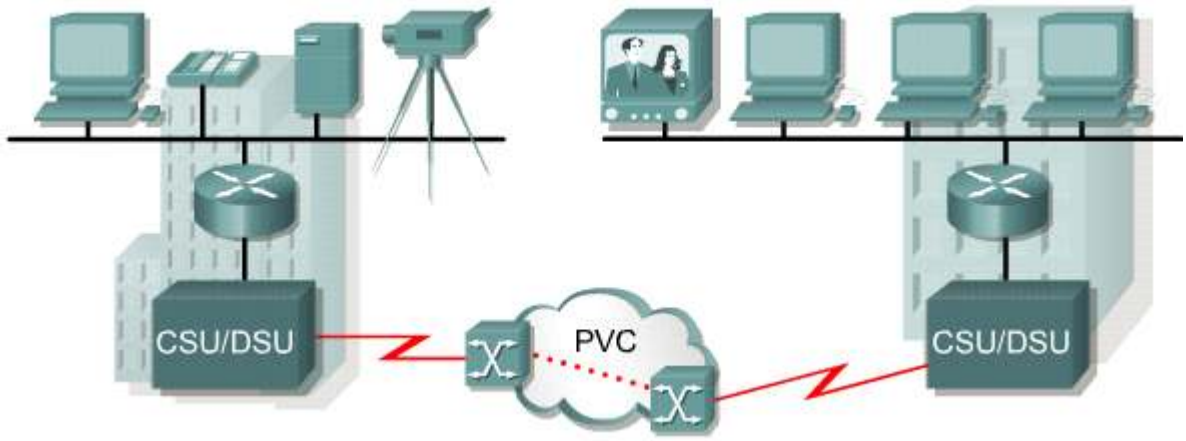
À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées à un circuit Frame Relay.

2.2 Technologies WAN

2.2.6 ATM

Les fournisseurs de communications ont déterminé qu'il existait un besoin de technologie réseau partagée permanente présentant peu de latence et de gigue à des débits bien plus élevés. La solution s'est présentée sous la forme du mode de transfert asynchrone

ATM (*Asynchronous Transfer Mode*). ATM offre des débits supérieurs à 155 Mbits/s. À l'instar des autres technologies partagées, telles que X.25 et Frame Relay, les diagrammes des WAN ATM ont le même aspect. 1



ATM est une technologie capable de transférer la voix, la vidéo et les données par des réseaux privés et publics. Elle est fondée sur une architecture à cellules, et non une architecture à trames. Les cellules ATM présentent toujours une longueur fixe de 53 octets. La cellule ATM de 53 octets contient une en-tête ATM de 5 octet, suivie de 48 octets de données utiles ATM. Les petites cellules de longueur fixe sont bien adaptées au transport du trafic vocal et vidéo, car ce trafic ne tolère pas les délais. En effet, le trafic vidéo et vocal n'a pas à attendre la fin de transmission d'un paquet de données de plus grande taille.

La cellule ATM de 53 octets est moins efficace que les trames et paquets de plus grande taille de Frame Relay et de X.25. Par ailleurs, la cellule ATM comporte au moins 5 octets de surcharge pour chaque ensemble de données utiles de 48 octets. Quand la cellule transporte des paquets de couche réseau segmentée, la surcharge est plus importante, car le commutateur ATM doit être en mesure de regrouper les paquets au niveau de la destination. Une ligne ATM typique nécessite un débit presque 20% plus important que celui de Frame Relay pour transporter le même volume de données de couche réseau.

ATM offre des circuits virtuels permanents et des circuits virtuels commutés, mais ces derniers sont plus courants avec les WAN.

Tout comme les autres technologies partagées, ATM accepte plusieurs circuits virtuels sur une seule connexion par ligne louée vers la périphérie du réseau.

Activité de média interactive

Case à cocher: Technologies WAN – ATM *(Asynchronous Transfer Mode)*

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées aux connexions ATM.

2.2 Technologies WAN

2.2.7 DSL

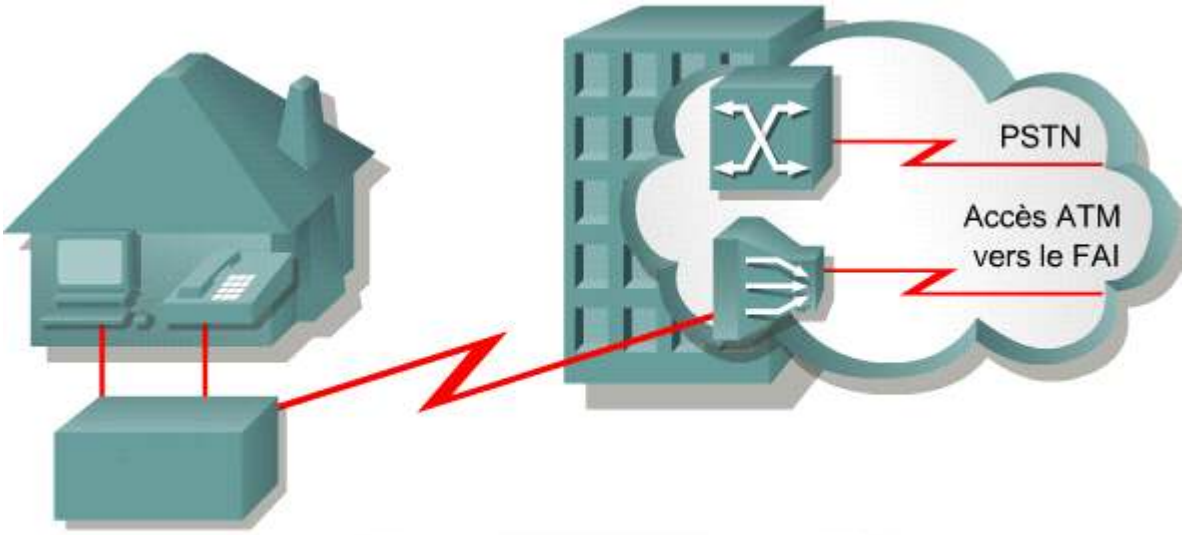
Le DSL (*Digital Subscriber Line*) est une technologie à large bande qui utilise les lignes téléphoniques à paire torsadée existantes pour transporter des données à large bande aux abonnés du service. On considère que le DSL est un service à large bande par rapport au service à bande de base des réseaux locaux typiques. Large bande désigne une technique utilisant plusieurs fréquences au sein d'un même support physique pour transmettre des données. Le terme xDSL désigne un nombre de technologies DSL similaires, mais en compétition: 1

Service	Télédéchargement	Téléchargement
ADSL	64 Kbits/s - 8.192 Mbits/s	16 Kbits/s - 640 Kbits/s
SDSL	1.544 Mbits/s - 2.048 Mbits/s	1.544 Mbits/s - 2.048 Mbits/s
HDSL	1.544 Mbits/s - 2.048 Mbits/s	1.544 Mbits/s - 2.048 Mbits/s
IDSL	144 Kbits/s	144 Kbits/s
CDSL	1 Mbits/s	16 Kbits/s - 160 Kbits/s

- ADSL (*Asymmetric DSL*)
- SDSL (*Symmetric DSL*)
- HDSL (*High Bit Rate DSL*)
- IDSL (*DSL RNIS*)
- CDSL *(Consumer DSL)*, également appelé DSL-lite ou G.lite

La technologie DSL permet au fournisseur d'accès de proposer des services de réseau haut débit à ses clients, au moyen de boucles locales de cuivre existantes. La technologie DSL permet d'utiliser la ligne de boucle locale pour les connexions téléphoniques normales, ainsi que pour une connexion toujours active offrant une connectivité instantanée au réseau. Plusieurs lignes d'abonnés DSL sont multiplexées en un lien unique à haute capacité au moyen d'un multiplexeur d'accès DSL (DSLAM) dans les locaux du fournisseur d'accès. Les DSLAM incorporent la technologie TDM pour agréger un grand nombre de lignes d'abonnés sur un support moins encombrant, généralement une connexion T3/DS3. Les technologies DSL actuelles utilisent des techniques complexes de codage et de modulation pour obtenir des débits pouvant s'élever à 8 192 Mbits/s.

Le canal vocal d'un téléphone standard occupe la plage de fréquences entre 330 Hz et 3,3 KHz. Une plage, ou fenêtre, de fréquences de 4 KHz est considérée comme le minimum requis pour n'importe quelle transmission vocale sur la boucle locale. Les technologies DSL effectuent les transmissions de données en aval et en amont à des fréquences supérieures à cette plage de 4 KHz. C'est cette technique qui permet aux transmissions vocales et de données de s'effectuer simultanément sur un service DSL.
2



La boucle locale connecte le répartiteur au DSLAM. La voix et les données utilisent des plages de fréquences distinctes.

Les deux types de technologies DSL de base sont le DSL asymétrique (ADSL) et le DSL symétrique (SDSL). Toutes les formes de services DSL entrent dans les catégories ADSL ou SDSL et il existe plusieurs variétés de chaque type. Le service asymétrique offre à l'utilisateur une bande passante supérieure pour le téléchargement vers l'utilisateur à celle du transfert d'information dans la direction opposée. Le service symétrique fournit la même capacité dans les deux sens.

Certaines technologies DSL n'acceptent pas l'utilisation d'un téléphone. Le SDSL est appelé « dry copper » (cuivre sec), parce qu'il n'a pas de tonalité et n'offre pas de service téléphonique sur la même ligne. Par conséquent, une ligne distincte est requise pour le service SDSL.

Les différentes variétés de DSL fournissent des bandes passantes différentes, avec des capacités supérieures à celles d'une ligne louée T1 ou E1. Les taux de transfert dépendent de la longueur effective de la boucle locale, ainsi que du type et de la condition de ses câbles. Pour fournir un service satisfaisant, la boucle doit être inférieure à 5,5 kilomètres. La disponibilité du DSL est loin d'être universelle et il existe une grande diversité de types, de normes et de normes en émergence. Il ne constitue pas un choix populaire pour les services informatiques d'entreprise desservant des télétravailleurs. En général, un abonné ne peut pas opter pour se connecter directement au réseau d'entreprise, mais doit tout d'abord passer par un fournisseur d'accès Internet (FAI). De ce point, une connexion IP vers l'entreprise est effectuée par Internet. Ceci occasionne donc des risques. Pour répondre à ces préoccupations de sécurité, les services DSL offrent la possibilité d'utiliser des connexions de réseau privé virtuel (VPN) vers un serveur VPN, généralement situé dans les locaux de l'entreprise.

Activité de média interactive

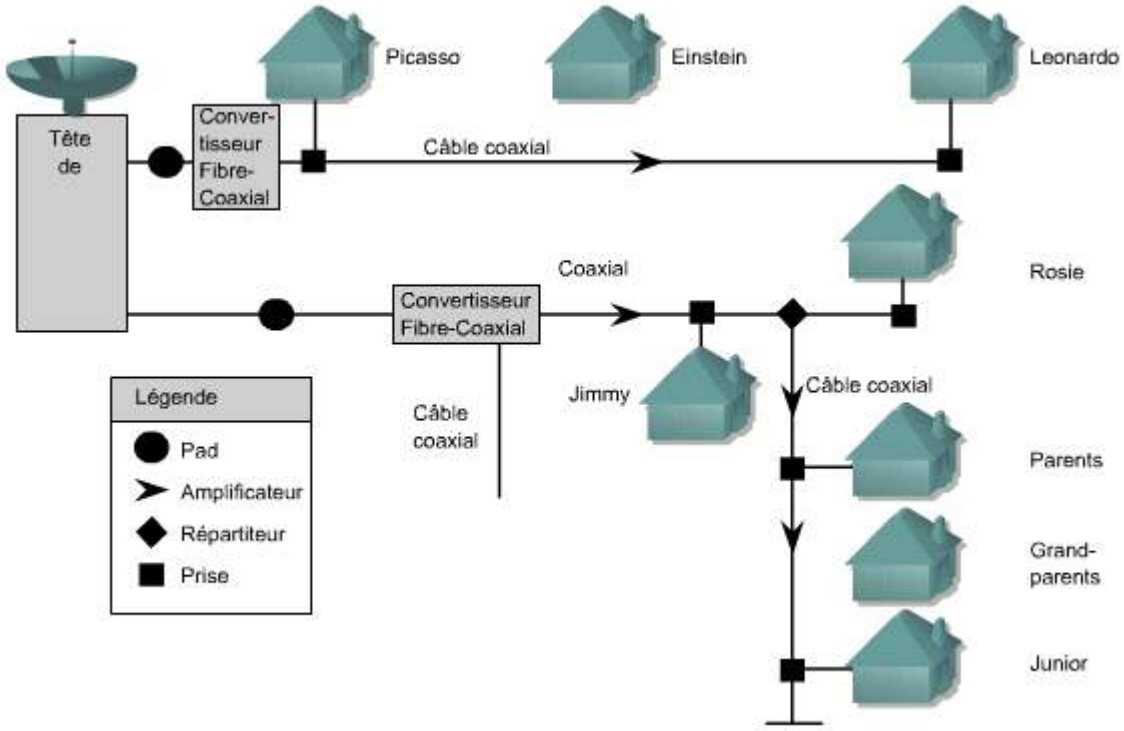
Case à cocher: Technologies WAN – DSL (*Digital Subscriber Line*)

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées aux connexions DSL.

2.2 Technologies WAN

2.2.8 Modem câble

Le câble coaxial est très répandu dans les zones urbaines pour distribuer des signaux de télévision. 1



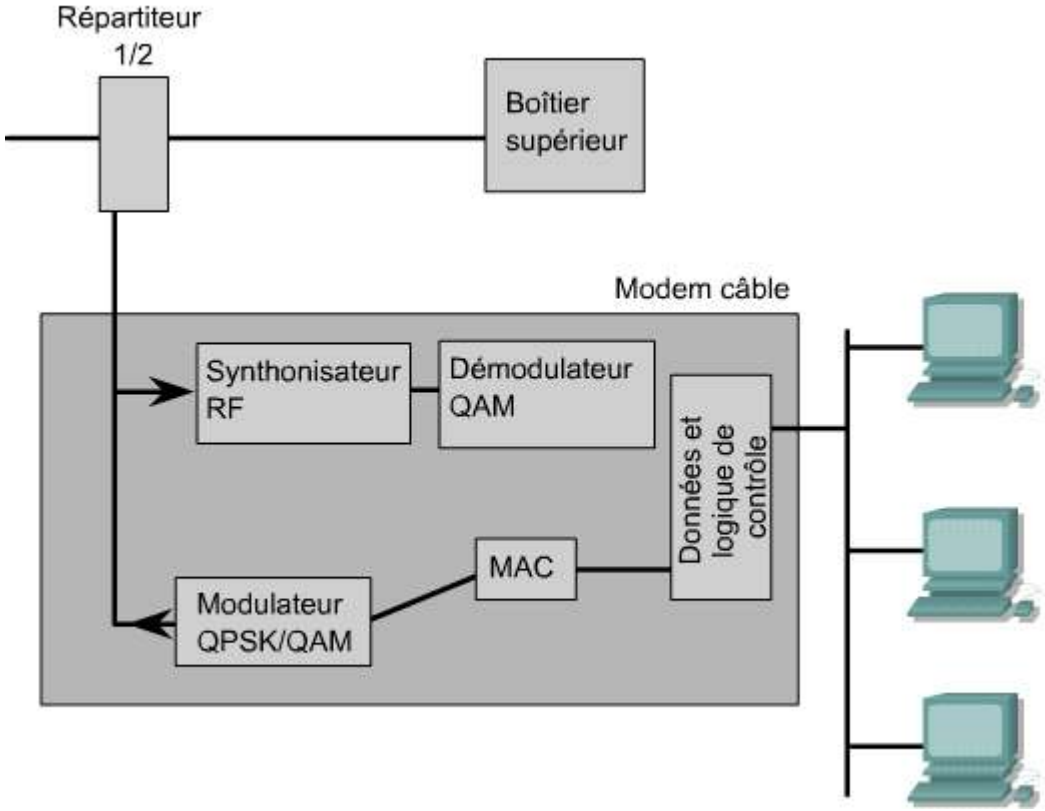
Un accès réseau est disponible sur certains réseaux de télévision câblée. Il offre une bande passante plus importante que la boucle locale téléphonique conventionnelle.

Les modems câble permettent d'effectuer des transmissions de données bidirectionnelles à haute vitesse sur les lignes coaxiales qui transmettent la télévision câblée. Certains fournisseurs d'accès câblé promettent des débits pouvant s'élever à 6,5 fois ceux de lignes louées T1. Cette vitesse fait du câble un support attrayant pour le transfert rapide de grandes quantités d'informations numériques, notamment des séquences vidéo, des fichiers audio ou des données en masse. Des informations dont le téléchargement prendrait deux minutes avec la technologie RNIS BRI peuvent être téléchargées en deux secondes par une connexion à modem câble.

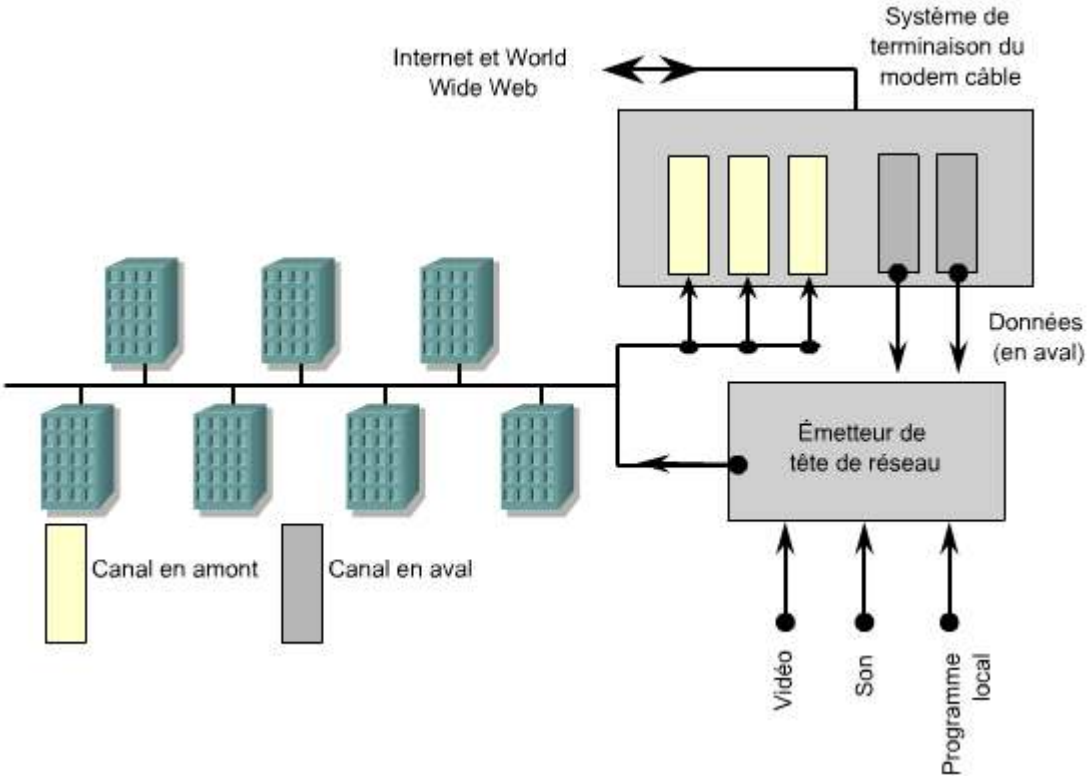
Les modems câbles offrent une connexion permanente et sont faciles à installer. La connexion permanente implique que les ordinateurs connectés peuvent être sujets à des intrusions à tout moment et qu'ils doivent donc être sécurisés par des pare-feu. Pour répondre à ces préoccupations de sécurité, les services à modem câble offrent la possibilité d'utiliser des connexions de réseau privé virtuel (VPN) vers un serveur VPN, généralement situé dans les locaux de l'entreprise.

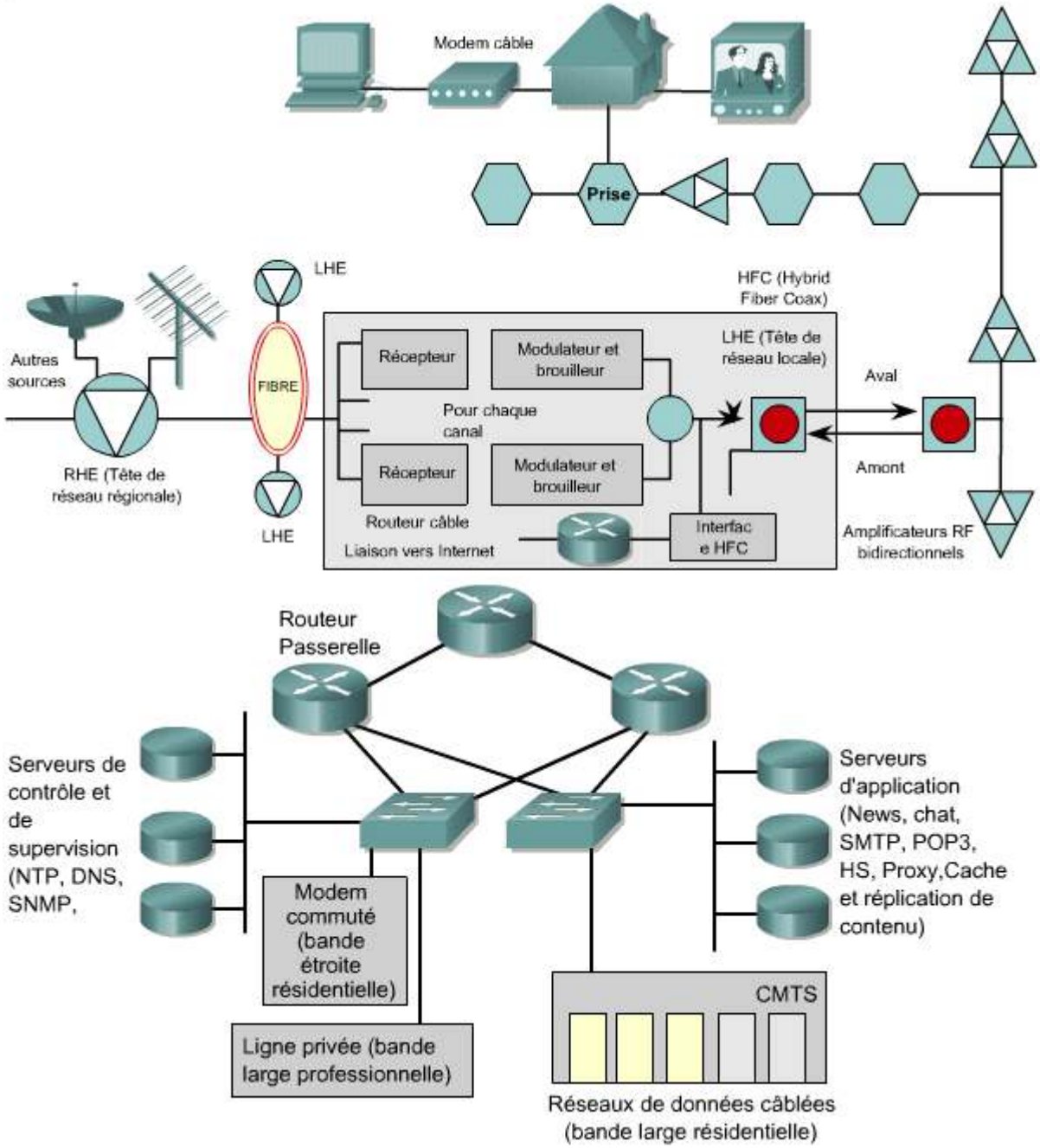
Un modem câble peut transférer jusqu'à 30 ou 40 Mbits/s de données sur un canal câblé à 6 MHz. Cela est pratiquement 500 fois plus rapide qu'un modem à 56 Kbits/s.

Avec un modem câble, un abonné peut continuer à recevoir son service de télévision câblée, tout en recevant des données sur un ordinateur personnel. Pour ce faire, il utilise un simple répartiteur à deux voies. 2



Les abonnés au modem câble doivent utiliser le FAI associé au fournisseur d'accès. Tous les abonnés locaux partagent la même bande passante. À mesure que des utilisateurs se joignent au service, la bande passante disponible peut être inférieure au débit attendu. [3]– [5]





Activité de média interactive

Case à cocher: Technologies WAN – Modems câble

À la fin de cette activité, l'étudiant sera en mesure d'identifier les caractéristiques associées aux modems câble.

2.3 Conception d'un WAN

2.3.1 Communication dans un réseau WAN

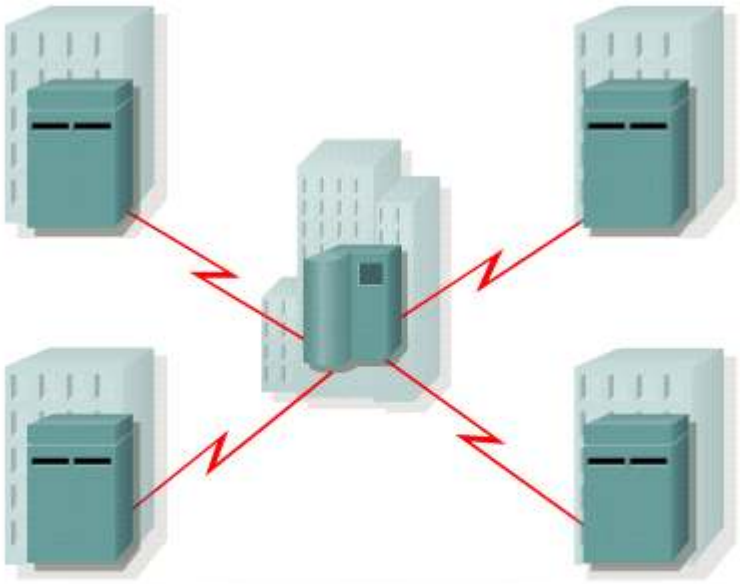
Les WAN sont considérés comme un jeu de liaison de données connectant des routeurs de réseaux locaux. Les stations d'extrémité et les serveurs de réseaux locaux échangent des données. Les routeurs transfèrent des données entre réseaux sur les liaisons de données.

Du fait du coût, ainsi que pour des raisons légales, un fournisseur d'accès ou un opérateur est généralement propriétaire des liaisons de données qui constituent un WAN. Les liaisons sont mises à la disposition des abonnés contre paiement, et sont utilisées pour interconnecter les réseaux locaux ou se connecter à des réseaux distants. Le taux de transfert des WAN (bande passante) est considérablement plus lent que les 100 Mbits/s que l'on trouve couramment sur les réseaux locaux. Les frais de mise en oeuvre des liaisons constituent l'élément de coût le plus important d'un WAN et l'objet de la conception doit être de fournir

une bande passante maximale à un prix acceptable. Du fait de pression exercée par les utilisateurs souhaitant obtenir davantage d'accès à des débits plus élevés et de celle exercée par la direction afin de réduire les coûts, il n'est pas aisé de déterminer la configuration WAN optimale.

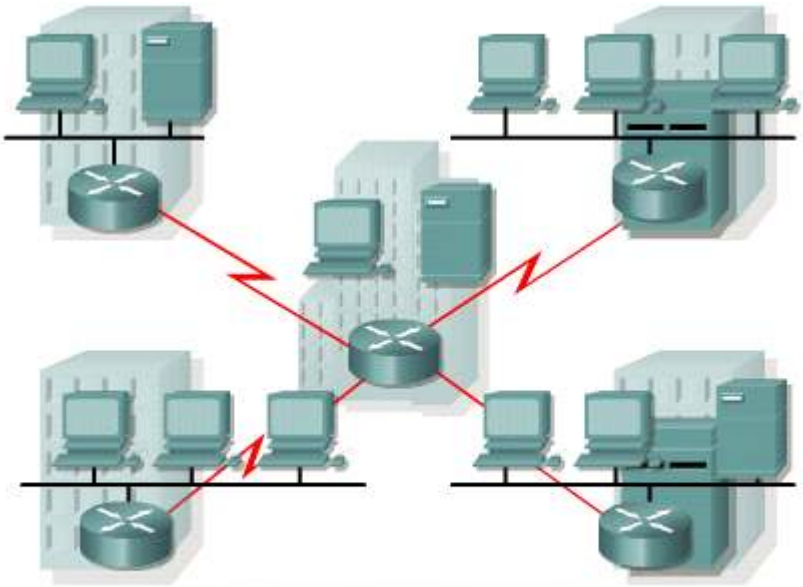
Les WAN transportent divers types de trafic, tels que les données, la voix et la vidéo. La conception sélectionnée doit fournir la capacité et les temps de transfert correspondant aux besoins de l'entreprise. Entre autres spécifications, il faut tenir compte de la topologie des connexions entre les différents sites, de la nature de ces connexions et de la bande passante.

Les WAN les plus anciens consistaient souvent en liaisons de données assurant la connexion à des ordinateurs centraux distants. 1



Les ordinateurs séparés par une certaine distance sont reliés par des lignes de communication de données.

Aujourd'hui, en revanche, les WAN relient des réseaux locaux séparés géographiquement. 2

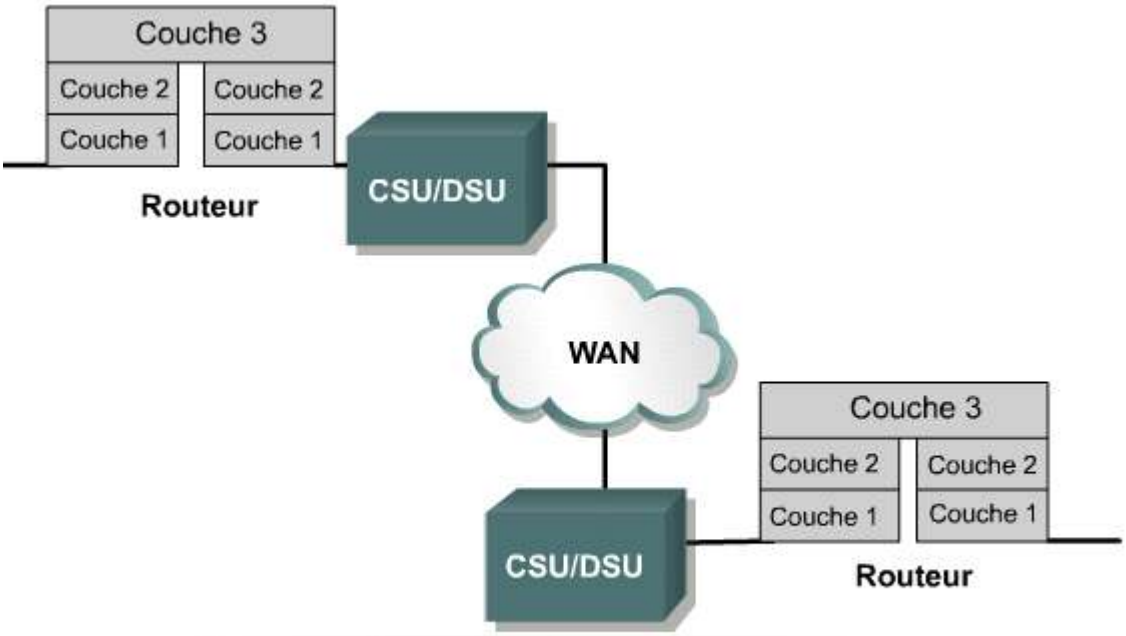


Les réseaux locaux séparés par une certaine distance sont reliés par des lignes de communication de données et des routeurs.

Les stations utilisateurs, les serveurs et les routeurs communiquent sur des réseaux locaux et les liaisons de données WAN se terminent au niveau des routeurs locaux. En échangeant des informations d'adresse de couche 3 sur les réseaux locaux

directement connectés, les routeurs déterminent le chemin le plus approprié sur le réseau pour les flux de données demandés. Les routeurs peuvent également effectuer une gestion par qualité de service, qui alloue des priorités aux différents flux de trafic.

Comme le WAN est un simple jeu d'interconnexions entre des routeurs de réseau local, il ne propose aucun service. Les technologies WAN fonctionnent au niveau des trois couches inférieures du modèle de référence OSI. 3



Les réseaux WAN fonctionnent aux trois niveaux inférieurs de la couche de protocoles OSI.

Des routeurs déterminent la destination des données à partir des en-têtes de la couche réseau et transfèrent les paquets à la connexion par liaison de données appropriée en vue de les livrer sur la connexion physique.

2.3 Conception d'un WAN

2.3.2 Étapes de conception d'un WAN

La conception d'un WAN peut s'avérer une activité complexe, mais une approche systématique peut aboutir à des performances élevées pour un coût réduit. De nombreux WAN ont évolué dans le temps et il se peut qu'un grand nombre des directives présentées ici n'aient pas été prises en compte. À chaque fois que la modification d'un WAN existant est envisagée, il est recommandé de suivre les étapes fournies dans le présent module. Les modifications d'un WAN peuvent survenir la suite de modifications telles qu'un développement de l'entreprise ou l'adoption de nouvelles pratiques ou méthodes de travail.

Les entreprises installent des WAN parce qu'il leur est nécessaire de déplacer des données rapidement entre différentes filiales. Le WAN est présent pour répondre aux besoins de l'entreprise. Cela implique des coûts, notamment pour la mise en oeuvre des équipements et la maintenance des liaisons de données.

Pour concevoir un WAN il est nécessaire de savoir quel trafic de données va être transporté, son origine et sa destination. Les WAN transportent une grande diversité de types de trafic, avec différents besoins relatifs à la bande passante, la latence et la gigue. 1

Trafic	Latence	Gigue	Bande passante
Voix	Basses	Basses	Moyen
Transactions (par exemple SNA)	Moyen	Moyen	Moyen
Courrier électronique	Hautes	Hautes	Hautes
Transfert de fichiers	Hautes	Hautes	Hautes
Données en lots	Hautes	Hautes	Hautes
Administration réseau	Hautes	Hautes	Basses
Vidéoconférence	Basses	Basses	Hautes

Certains types de trafic WAN avec leurs tolérances à la latence et la gigue, ainsi que leur demande en bande passante

Pour chaque paire de points d'extrémité et pour chaque type de trafic, il est nécessaire d'obtenir des informations sur les diverses caractéristiques de trafic. 2

- Connectivité et flux des volumes
- Données client-serveur
- Connexion ou orientation datagramme
- Tolérance à la latence, y compris sa durée et sa variabilité
- Tolérance à la disponibilité du réseau
- Tolérance au taux d'erreurs
- Priorité
- Type de protocole
- Longueur moyenne de paquet

Caractéristiques du trafic entre chaque paire de points d'extrémité

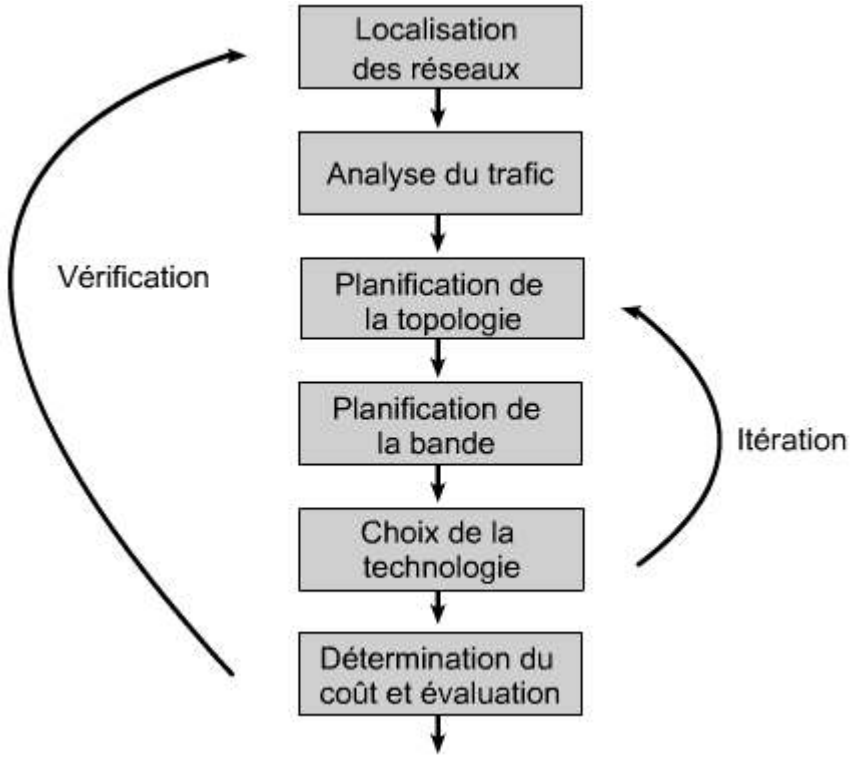
Ceci implique des analyses approfondies, ainsi que la consultation des utilisateurs du réseau. La conception consiste souvent à effectuer des mises à niveau, des extensions ou des modifications d'un WAN existant. Une grande partie des données nécessaires peut provenir des statistiques de gestion du réseau existant.

La connaissance des divers points d'extrémité permet de sélectionner une topologie ou une configuration pour le réseau. La topologie est influencée par des considérations géographiques, mais également par d'autres besoins, tels que la disponibilité. Une grande disponibilité demande des liaisons supplémentaires offrant des chemins de données supplémentaires pour la redondance et l'équilibrage de la charge.

Lorsque les points d'extrémité et les liaisons ont été choisis, la bande passante nécessaire peut être estimée. Le trafic sur les liaisons peut présenter divers besoins en matière de latence et de gigue. Une fois la disponibilité de la bande passante déterminée, des technologies de liaison appropriées doivent être sélectionnées.

Enfin, les coûts d'installation et d'exploitation du WAN peuvent être déterminés et comparés aux besoins de l'entreprise ayant nécessité l'installation du WAN.

En pratique, les étapes présentées à la figure 3



constituent rarement un processus linéaire. Plusieurs modifications peuvent s'avérer nécessaires avant la finalisation d'une conception. Il est également nécessaire d'effectuer une surveillance et une réévaluation constantes après l'installation du WAN, afin de maintenir des performances optimales.

Activité de média interactive

Glisser-Positionner: Étapes de conception d'un WAN

À la fin de cette activité, l'étudiant sera en mesure d'identifier les étapes élémentaires de conception d'un WAN.

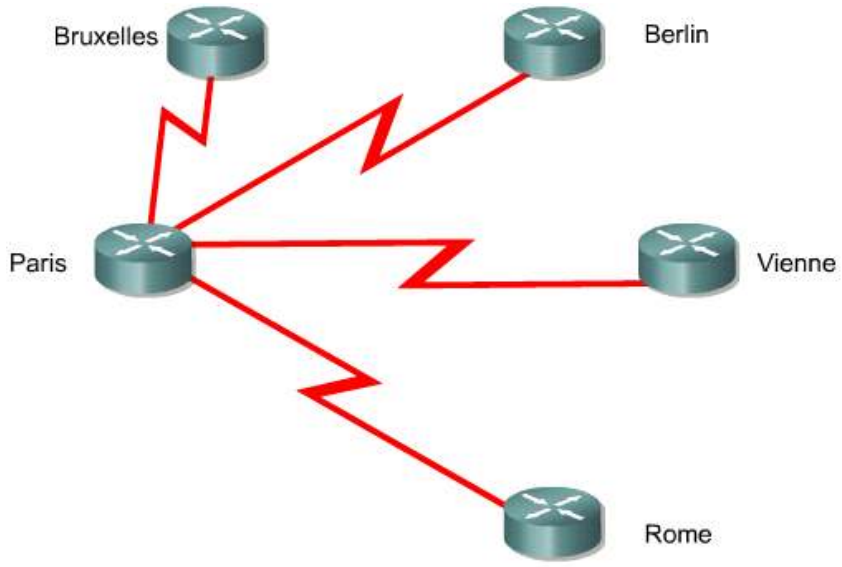
2.3 Conception d'un WAN

2.3.3 Identification et sélection des fonctionnalités du réseau

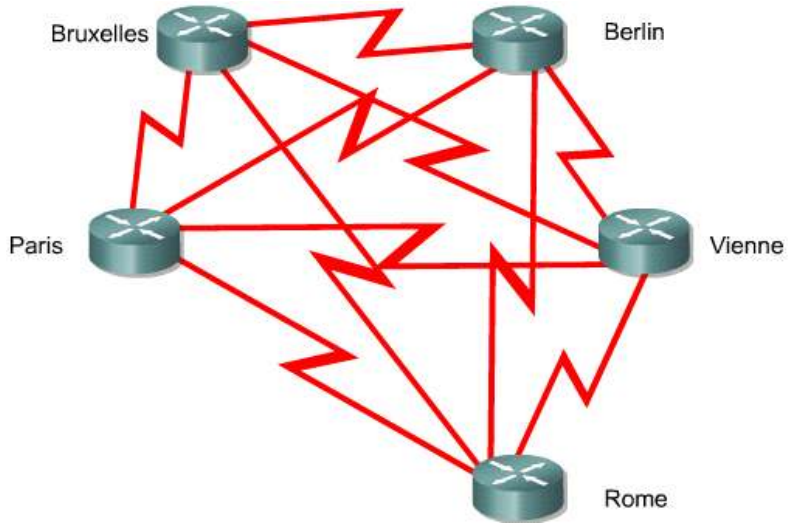
La conception d'un WAN implique les activités suivantes:

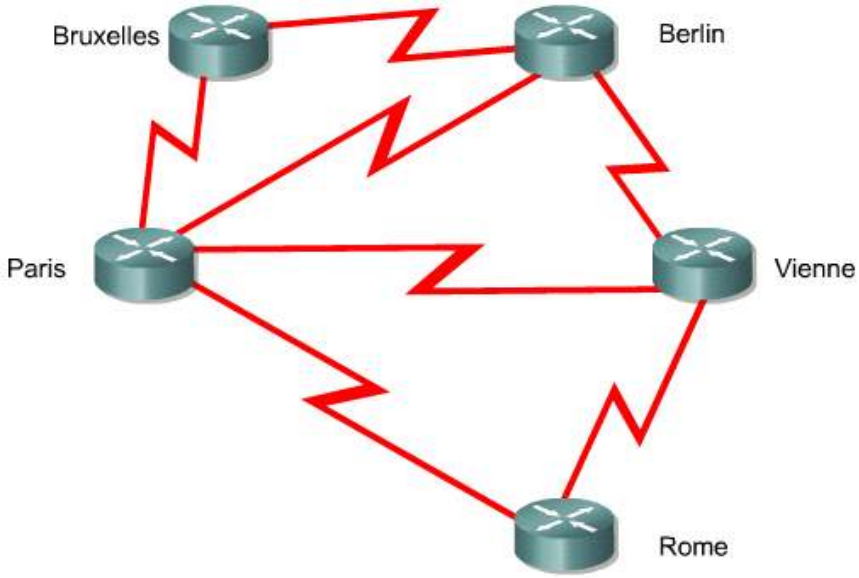
- La sélection d'un motif ou d'une configuration d'interconnexion entre les divers sites
- La sélection des technologies permettant à ces liaisons de répondre aux besoins de l'entreprise à un coût acceptable

De nombreux WAN s'appuient sur une topologie en étoile. À mesure de la croissance de l'entreprise et de l'apparition de nouvelles filiales, ces dernières sont connectées au siège pour produire une topologie en étoile traditionnelle. [1]



Les points d'extrémité de l'étoile sont parfois interconnectés, en une topologie maillée ou à maillage partiel. [2] [3]





Ceci offre de nombreuses combinaisons possibles d'interconnexion. Lors de la conception, de la réévaluation ou de la modification d'un WAN, il est nécessaire de sélectionner une topologie répondant aux besoins de la conception.

Pour la sélection d'une configuration, plusieurs facteurs doivent être pris en compte. Un nombre plus important de liaisons augmente le coût des services de réseau, alors que plusieurs chemins entre les destinations augmentent la fiabilité. En revanche,

l'ajout d'équipements de réseau sur le chemin des données augmente la latence et réduit la fiabilité. En général, chaque paquet doit être entièrement reçu par un nœud avant d'être transmis au suivant. Il existe de nombreuses technologies dédiées présentant différentes fonctionnalités pour les liaisons de données. 4

Technologie	Charge	Débit binaire maximum	Autre
Ligne louée	Distance, capacité	Illimitée	Capacité fixe permanente
Service téléphonique	Distance, durée	33-56kbits/s	Accès commuté, connexion lente
RNIS	Distance, capacité	64 or 128 kbits/s <2 Mbps, PRI	Accès commuté, connexion rapide
X.25	Volume	<48 kbits/s	Commuté capacité fixe
ATM	Capacité	>155 Mbits/s	Capacité variable permanente

Les technologies qui demandent l'établissement d'une connexion avant que les données ne puissent être transmises, tels que le téléphone analogique, le RNIS ou X.25 ne sont pas adaptées aux WAN qui nécessitent des temps de réponse rapides ou une faible latence. Une fois établis, RNIS et d'autres services commutés constituent des circuits à faible latence présentant peu de gigue. RNIS constitue souvent le meilleur choix pour connecter un réseau de petit bureau/bureau à domicile au réseau d'entreprise et fournir une connectivité fiable, ainsi qu'une bande passante adaptable. Contrairement au câble et au DSL, RNIS constitue une option valable quand un service téléphonique moderne est présent. RNIS s'avère également utile comme liaison de secours pour les connexions primaires, ainsi que pour fournir des connexions à bande passante à la demande, parallèles à une connexion primaire. Ces technologies offrent l'avantage de n'être payantes que lorsque le circuit est utilisé.

Les différentes parties de l'entreprise peuvent être connectées directement au moyen de lignes louées, ou peuvent être connectées à l'aide d'une liaison d'accès au point de présence le plus proche d'un réseau partagé. X.25, Frame Relay et ATM sont des exemples de réseaux partagés. Les lignes louées sont généralement bien plus longues, et donc bien plus coûteuses que les liaisons d'accès, mais peuvent pratiquement offrir n'importe quel débit. Elles présentent également des niveaux très faibles de latence et de gigue.

Les réseaux ATM, Frame Relay et X.25 peuvent transporter du trafic provenant de plusieurs clients sur les mêmes liaisons internes. L'entreprise n'a aucun contrôle sur le nombre de liaisons ou de sauts que les données doivent traverser sur le réseau partagé. Elle ne peut pas contrôler la durée d'attente des données au niveau de chaque nœud avant le passage à la liaison suivante. Ces niveaux incertains de latence et de gigue rendent ces technologies peu adaptées à certains types de trafic réseau. Toutefois, les inconvénients d'un réseau partagés sont souvent compensés par ses coûts réduits. Comme plusieurs clients partagent la liaison, les coûts qui incombent à chacun d'entre eux sont généralement inférieurs à ceux d'une liaison directe de même capacité.

Bien qu'ATM soit un réseau partagé, il a été conçu pour produire des niveaux minimes de latence et de gigue grâce à des liaisons internes à haute vitesse permettant de transférer des unités de données faciles à gérer, les cellules. Les cellules ATM ont une longueur fixe de 53 octets ; 48 pour les données et 5 pour l'en-tête. ATM sert largement à transporter du trafic sensible aux attentes. Le Frame Relay peut également être utilisé pour le trafic sensible aux attentes, souvent associé à des mécanismes QoS permettant de donner la priorité aux données les plus sensibles.

Un WAN typique utilise une combinaison de technologies généralement choisies en fonction du type et du volume de trafic. Les technologies RNIS, DSL, Frame Relay ou les lignes louées sont utilisées pour connecter les filiales individuelles à une zone. Le Frame Relay, ATM ou les lignes louées permettent de reconnecter les zones externes au backbone. ATM ou les lignes louées constituent le backbone du WAN.

2.3 Conception d'un WAN

2.3.4 Modèle de conception à trois couches

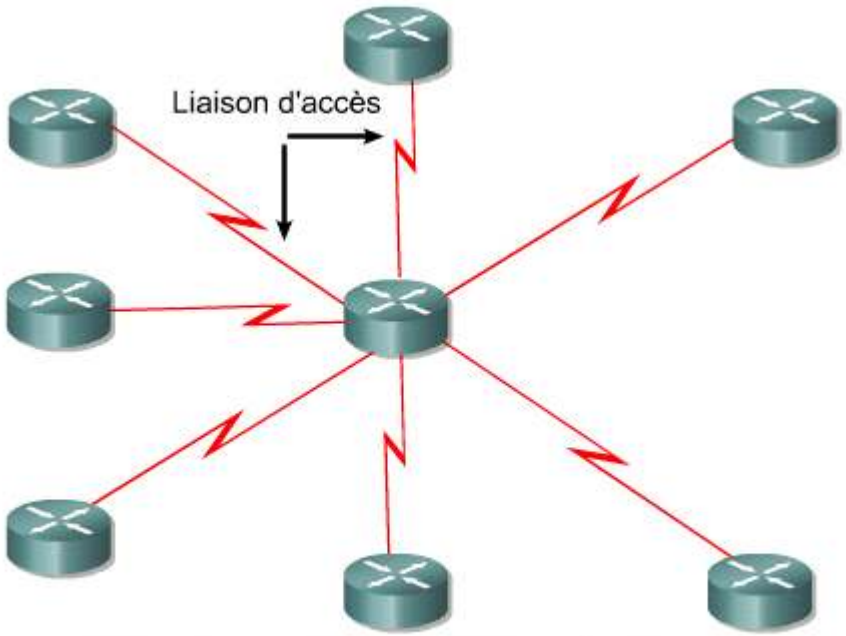
Une approche systématique s'avère nécessaire quand un grand nombre de sites doivent être contactés. Une solution hiérarchique à trois couches offre de nombreux avantages. 1

Évolutivité	Les réseaux créés selon le modèle hiérarchique peuvent connaître une croissance plus forte, sans effet négatif sur le contrôle et la facilité de gestion, parce que les fonctionnalités sont localisées et qu'il est plus facile de détecter les problèmes éventuels. Le réseau téléphonique public commuté est un exemple de réseau hiérarchique à très grande
Facilité de mise en œuvre	Puisqu'un modèle hiérarchique attribue des fonctionnalités précises à chaque couche, la mise en œuvre du réseau s'en trouve facilitée.
Facilité de dépannage	Les fonctions de chaque couche étant clairement définies, il devient plus facile d'isoler les problèmes qui peuvent survenir sur le réseau. Il est également plus facile de segmenter temporairement le réseau pour réduire l'étendue d'un problème.
Prévisibilité	Le comportement d'un réseau s'appuyant sur des couches fonctionnelles est assez prévisible, ce qui facilite considérablement la planification de la croissance. Cette conception facilite la modélisation des performances du réseau à des fins d'analyse.
Prise en charge des protocoles	La combinaison d'applications et de protocoles actuels et futurs est beaucoup plus facile sur des réseaux créés selon un modèle hiérarchique, en raison de l'organisation logique de l'infrastructure sous-jacente.
Facilité de gestion	Tous les avantages énumérés ci-dessus rendent le réseau plus facile à gérer.

Imaginons une entreprise opérationnelle dans chaque pays de l'Union Européenne et disposant d'une filiale dans chaque ville de plus de 10 000 habitants. Chaque filiale a un réseau et il a été décidé d'interconnecter les filiales. Un réseau maillé n'est évidemment pas réalisable, car un nombre de liaisons proche de 500 000 serait nécessaire pour les 900 centres. Une étoile simple sera difficile à mettre en oeuvre, car elle nécessite un routeur disposant de 900 interface au niveau du concentrateur ou d'une interface unique transportant 900 circuits virtuels vers un réseau à commutation de paquets.

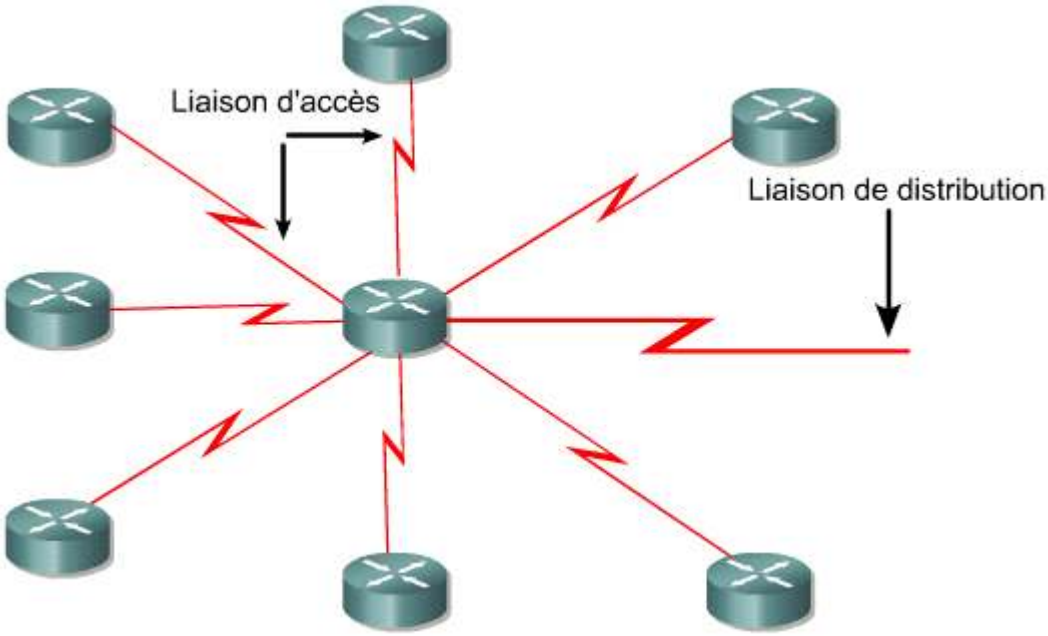
Au lieu de cela, envisagez plutôt un modèle de conception hiérarchique. Les réseaux regroupés dans une zone sont interconnectés, plusieurs zones sont interconnectées pour constituer une région et les diverses régions sont interconnectées pour former le noyau du WAN.

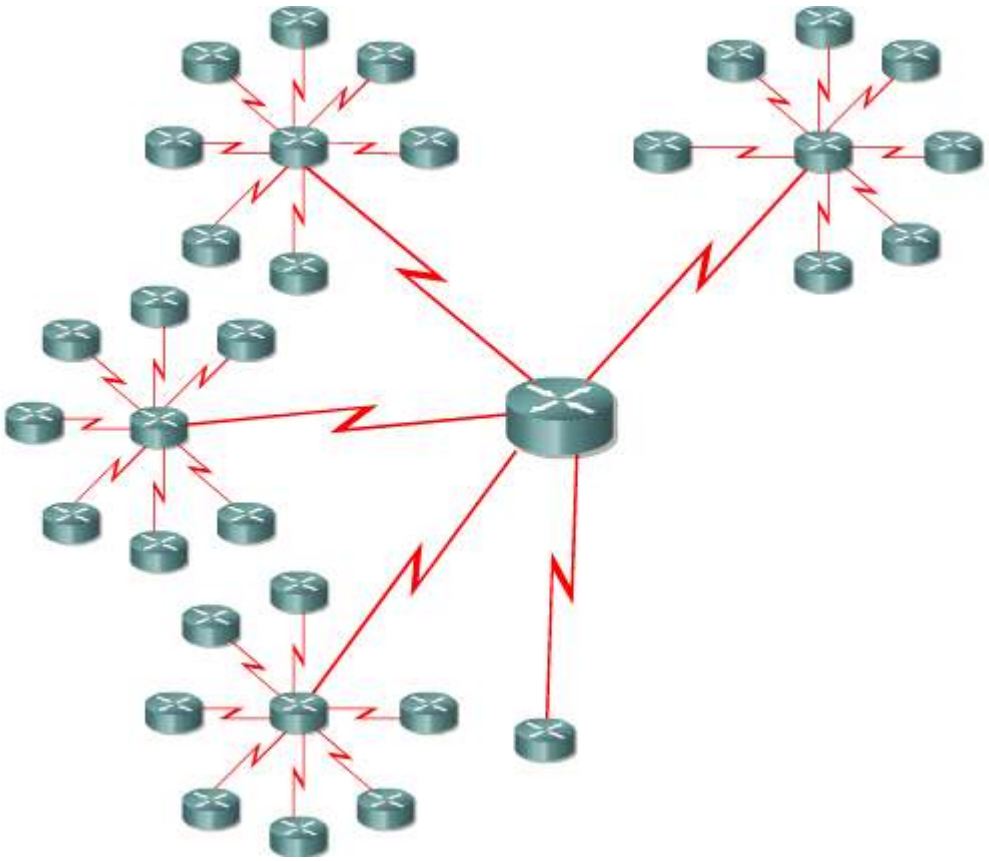
La zone peut être fondée sur le nombre de sites à connecter, avec une limite supérieure d'entre 30 et 50. La zone peut adopter une topologie en étoile, 2



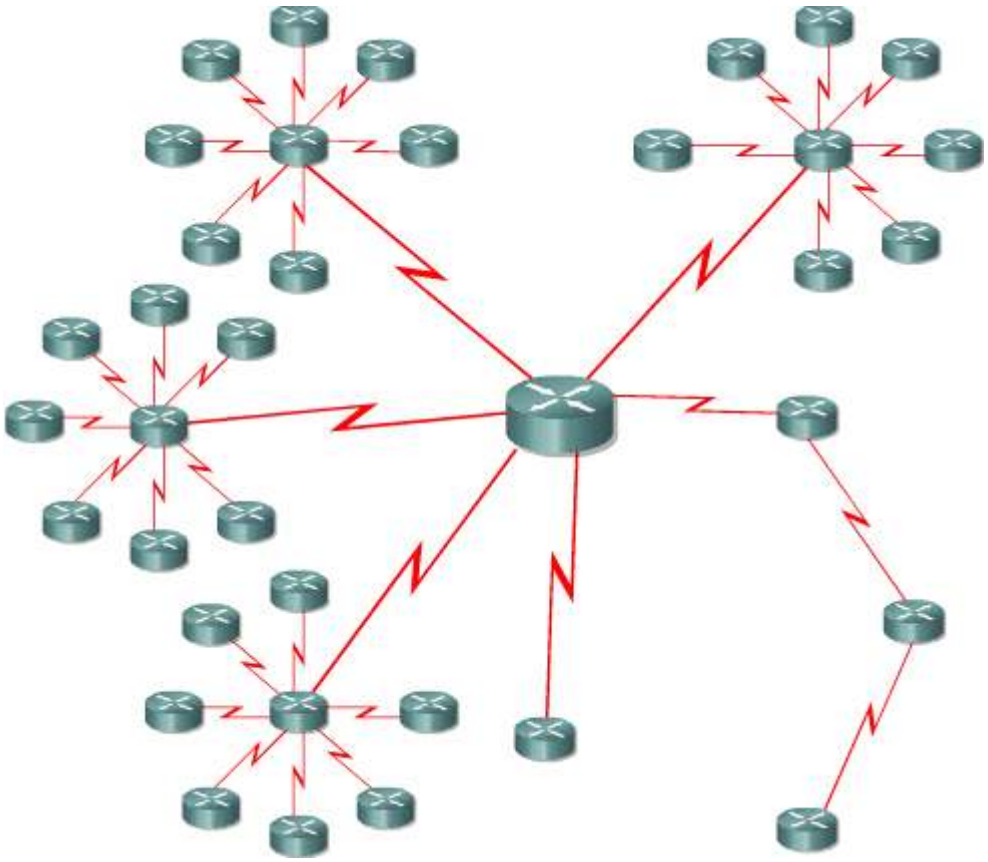
Les réseaux locaux d'une zone sont connectés en étoile.

les concentrateurs des étoiles étant reliés pour former la région. 3 4





Les régions peuvent être géographiques et connecter entre trois et dix zones, le noyau de chaque région pouvant être relié en point-à-point.



Ce modèle à trois couches suit la conception hiérarchique utilisée pour les systèmes téléphoniques. Les liaisons qui connectent les divers sites d'une zone et qui fournissent un accès au réseau d'entreprise prennent le nom de liaisons d'accès ou de couche d'accès du WAN. Le trafic entre les zones est distribué par les liaisons de distribution et se voit déplacé vers les liaisons du noyau pour le transfert vers d'autres régions lorsque cela s'avère nécessaire.

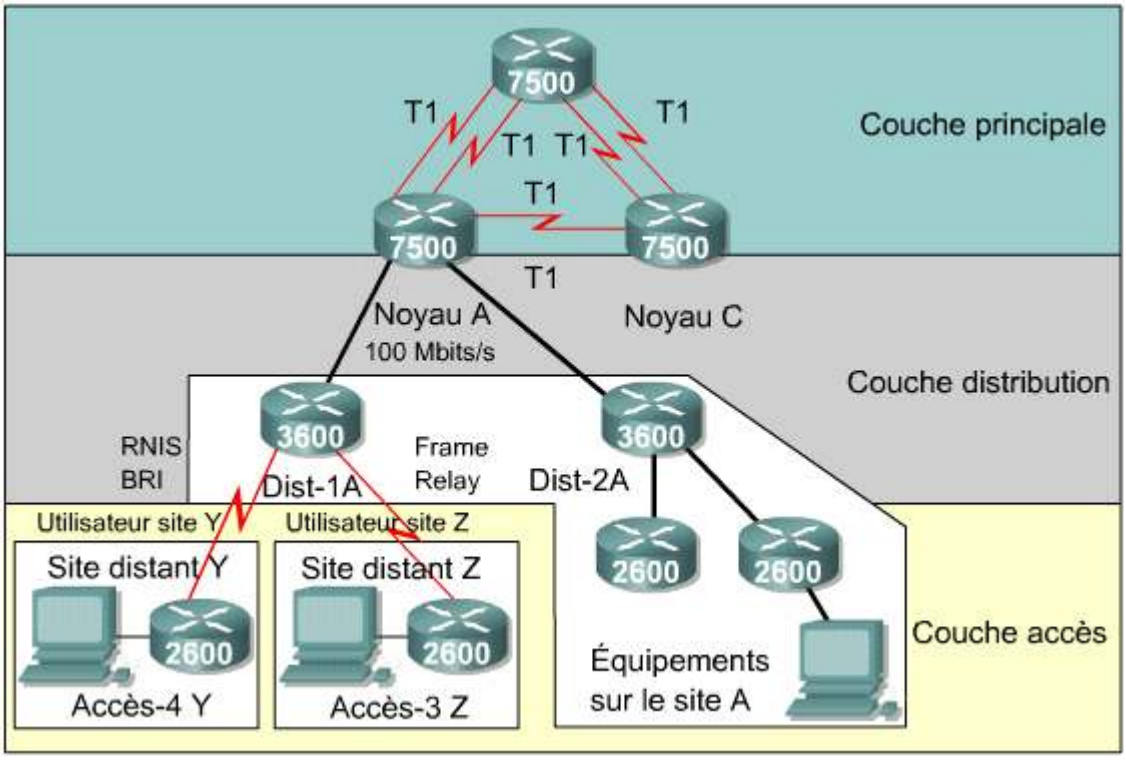
Cette hiérarchie s'avère souvent utile quand le trafic du réseau reproduit la structure de filiales de l'entreprise et est divisé en régions, zones et filiales. Elle est également utile quand il existe un service central auquel toutes les filiales doivent avoir accès, mais que les niveaux de trafic sont insuffisants pour justifier la connexion directe d'une filiale au service.

Le réseau local situé au centre de la zone peut disposer de nombreux serveurs fournissant des services au niveau de la zone et au niveau local. En fonction des volumes et des types de trafic, les connexions d'accès peuvent être commutées, louées ou de type Frame Relay. La technologie Frame Relay facilite le maillage pour la redondance, sans demander l'ajout de connexions physiques supplémentaires. Les liaisons de distribution peuvent être de technologie Frame Relay ou ATM et le noyau du réseau peut être une ligne ATM ou louée.

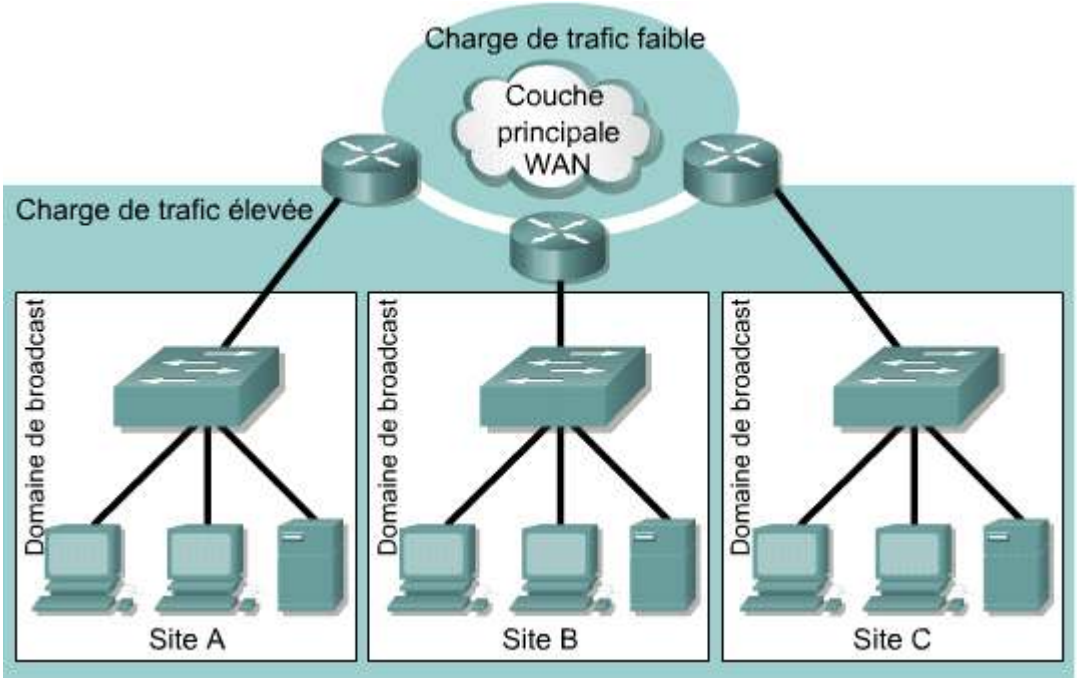
2.3 Conception d'un WAN

2.3.5 Autres modèles à conception en couches

De nombreux réseaux ne nécessitent pas la complexité d'une hiérarchie à trois couches complète. 1



Il est possible d'utiliser des hiérarchies plus simples. 2



Une entreprise disposant de plusieurs filiales relativement petites et nécessitant un trafic inter-filiales minimum peut choisir une conception en une couche. Historiquement, cette solution n'a jamais connu de succès, du fait de la longueur des lignes louées. Lorsque les coûts ne sont pas liés à la distance, la technologie Frame Relay rend aujourd'hui cette solution envisageable.

S'il existe un besoin de concentration géographique, une conception a deux niveaux s'avère appropriée. Ceci produit un motif en «étoile des étoiles». Ici encore, ce modèle, fondé sur la technologie des lignes louées, est considérablement différent de celui fondé sur la technologie Frame Relay.

Lors de la planification de réseaux plus simples, le modèle à trois couches doit toujours être envisagé, car il offre une meilleure évolutivité au réseau. Le concentrateur situé au centre d'un modèle à deux couches constitue également un noyau, mais sans que d'autres routeurs noyaux n'y soient connectés. De même, avec une solution à une seule couche, le concentrateur de zone sert de concentrateur régional et de concentrateur noyau. Cela permet une croissance future facile et rapide, la conception de base pouvant être répliquée pour y ajouter de nouvelles zones de service.

2.3 Conception d'un WAN

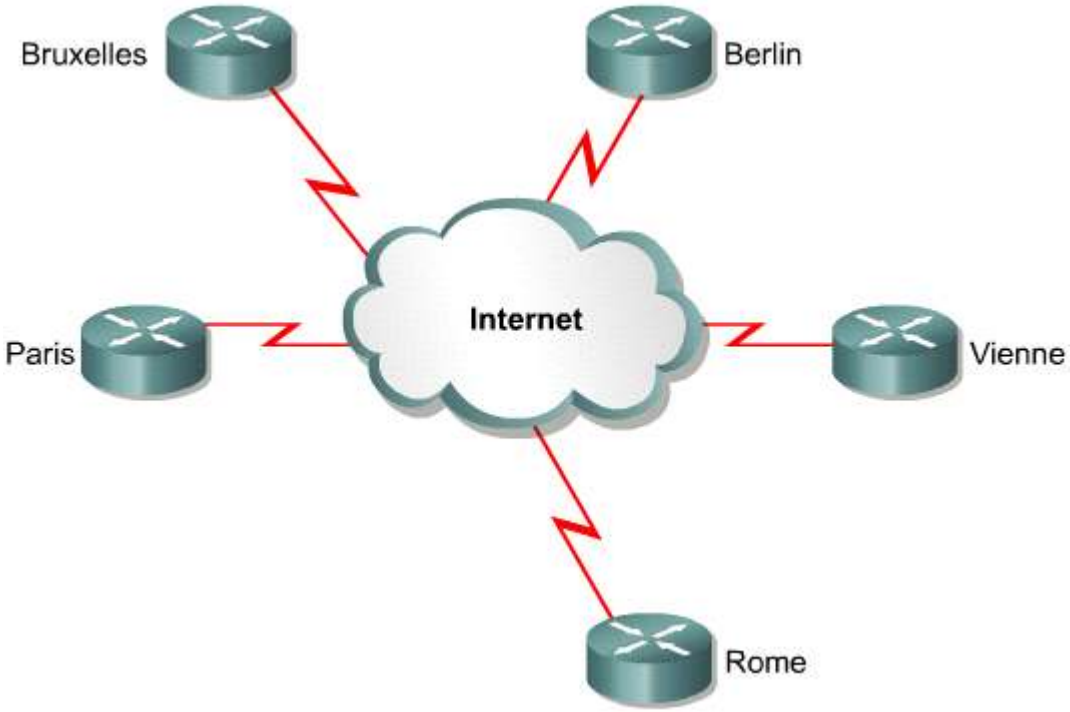
2.3.6 Autres considérations liées à la conception de WAN

De nombreux WAN d'entreprise ont des connexions à Internet. Ceci pose des problèmes de sécurité, mais offre également d'autres possibilités pour le trafic inter-filiales.

La partie du trafic qui doit être prise en compte lors de la conception se dirige vers Internet ou en provient. Comme Internet est probablement présent sur tous les sites où l'entreprise dispose d'un réseau local, il existe principalement deux méthodes pour transporter ce trafic. Chaque réseau local peut avoir une connexion à son FAI local, ou il peut exister une connexion unique de l'un des routeurs noyaux au FAI. La première méthode offre l'avantage de transporter le trafic sur Internet et non sur le réseau de l'entreprise, ce qui mène vraisemblablement à des liaisons WAN moins étendues. L'inconvénient de ces liaisons multiples est que l'ensemble du WAN de l'entreprise est vulnérable à des attaques provenant d'Internet. Il est également difficile de surveiller et de sécuriser les nombreux points de connexion. Un point de connexion unique est en effet bien plus facile à surveiller et à sécuriser, même si cela oblige le WAN de l'entreprise à transporter du trafic qui aurait autrement été transmis sur Internet.

Si chaque réseau local de l'entreprise a une connexion Internet séparée, une autre possibilité s'ouvre pour le WAN. Lorsque les volumes de trafic sont relativement faibles, Internet peut servir de WAN d'entreprise et transporter tout le trafic inter-filiales. La sécurité des divers réseaux locaux représente un problème, mais l'économie réalisée sur les connexions du WAN peut payer la sécurité.

Les serveurs doivent être placés le plus près possible des sites qui vont y accéder le plus souvent. La réplication des serveurs, avec des dispositions prises pour des mises à jour inter-serveur pendant les périodes creuses, réduit le nombre de liaisons requises. L'emplacement des services accessibles depuis Internet est fonction de la nature du service, du trafic anticipé et des questions de sécurité. Cette spécialisation de la conception sort toutefois du programme de ce cours.



Résumé

La compréhension des points clés suivants devrait être acquise:

- La différence entre les zones géographiques desservies par des réseaux étendus (WAN) et des réseaux locaux (LAN)
- Les similitudes des couches du modèle OSI existant entre les WAN et les LAN
- La familiarisation avec la terminologie WAN décrivant l'équipement, par exemple CPE, CO, boucle locale, ETTD, ETCD, CSU/DSU et TA
- La familiarisation avec la terminologie WAN décrivant les services et les normes, telle que RNIS, Frame Relay, ATM, T1, HDLC, PPP, POST, BRI, PRI, X.25 et DSL
- Les différences entre les réseaux à commutation de paquets et à commutation de circuits
- Les différences et similitudes entre les technologies WAN actuelles, notamment les services analogiques commutés, RNIS, lignes louées, X.25, Frame Relay et ATM
- Les avantages et les inconvénients des services DSL et modem câble
- La propriété et le coût associés aux liaisons de données WAN
- Les besoins en matière de capacité et de temps de transfert pour les différents types de WAN, tels que la voix, les données et la vidéo
- La familiarisation avec les topologies WAN, telles que point-à-point, en étoile et maillée
- Les éléments de conception d'un WAN, notamment la mise à niveau, l'extension, la modification d'un WAN existant, ou la recommandation d'un service WAN à une entreprise en fonction de ses besoins
- Les avantages offerts par une conception hiérarchique de WAN à trois couches
- Les autres possibilités de trafic WAN inter-filiales

Résumé

- Un réseau WAN est un réseau de communication de données qui fonctionne au-delà de la portée géographique d'un réseau LAN.
- Les WAN utilisent le modèle de référence OSI, mais se concentrent principalement sur la couche 1 et la couche 2. Les normes WAN décrivent généralement les méthodes de livraison sur la couche physique et les caractéristiques requises pour la couche de liaison de données, notamment l'adressage physique, le contrôle de flux et l'encapsulation.
- Les réseaux à commutation de paquets ont été développés pour éviter les dépenses entraînées par les réseaux à commutation de circuits publics et pour offrir une technologie WAN plus économique.
- Les technologies et les normes WAN sont notamment les suivantes : RNIS, Frame Relay, ATM, T1, HDLC, PPP, POST, BRI, PRI, X.25 et DSL.
- Pour concevoir un WAN il est nécessaire de savoir quel trafic de données va être transporté, son origine et sa destination. Les WAN transportent une grande diversité de types de trafic, avec différents besoins relatifs à la bande passante, la latence et la gigue.
- La conception d'un WAN implique les activités suivantes :
  - La sélection d'un motif ou d'une configuration d'interconnexion entre les divers sites
  - La sélection des technologies permettant à ces liaisons de répondre aux besoins de l'entreprise à un coût acceptable

Vue d'ensemble

Ce module offre une vue d'ensemble des technologies WAN. Il présente et explique des technologies telles que la transmission série, le multiplexage temporel (TDM - *Time-Division Multiplexing*), la démarcation, l'équipement terminal de traitement de données (ETTD) et l'équipement de communication de données (ETCD). Le développement et l'utilisation de l'encapsulation HDLC (*high-level data link control*), ainsi que des méthodes de configuration et de dépannage d'une interface série sont présentés.

PPP (Protocole point-à-point) est le meilleur protocole à mettre en oeuvre sur une connexion commutée WAN série. Il gère les communications synchrones et asynchrones et fournit des fonctions de détection d'erreurs. Mais surtout, il comporte un processus d'authentification par CHAP ou PAP. Il peut être utilisé sur différents médias physiques, notamment les câbles à paires torsadées, la fibre optique ou la transmission par satellite.

Ce module décrit les procédures de configuration de PPP, ainsi que les options disponibles et les concepts de dépannage. PPP offre notamment la possibilité d'utiliser l'authentification PAP ou CHAP.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Expliquer les communications série
- Décrire et donner un exemple de multiplexage temporel (TDM)
- Identifier le point de démarcation d'un réseau WAN
- Décrire les fonctions des ETTD et des ETCD
- Discuter du développement de l'encapsulation HDLC
- Utiliser la commande **`encapsulation hdlc`** pour configurer HDLC
- Dépanner une interface série avec les commandes **`show interface`** et **`show controllers`**
- Identifier les avantages de PPP
- Expliquer les fonctions des composants LCP (*Link Control Protocol*) et NCP (Network Control Protocol) de PPP
- Décrire les différentes parties d'une trame PPP
- Identifier les trois phases d'une session PPP
- Expliquer la différence entre PAP et CHAP
- Énumérer les étapes du processus d'authentification PPP
- Identifier les diverses options de configuration de PPP
- Configurer l'encapsulation PPP
- Configurer l'authentification CHAP et PAP
- Utiliser la commande **`show interface`** pour vérifier l'encapsulation série
- Résoudre les problèmes de configuration de PPP à l'aide de **`debug PPP`**

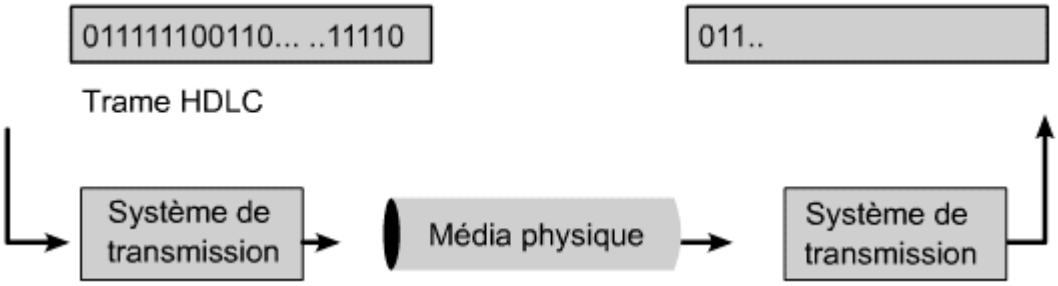
À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
3.1	Liaisons série point-à-point
3.2	Authentification PPP
3.3	Configuration de PPP

3.1 Liaisons série point-à-point

3.1.1 Présentation des communications série

Les technologies des réseaux WAN s'appuient sur une transmission série au niveau de la couche physique. Cela signifie que les bits d'une trame sont transmis un par un sur le support physique.

Les bits qui constituent la trame de couche 2 sont signalés un par un par les processus de la couche physique s'effectuant sur le support physique. 1



Les méthodes de signalisation sont notamment NRZ-L (*Nonreturn to Zero Level*), HDB3 (*High Density Binary 3*) et AMI (Alternative Mark Inversion). Il ne s'agit que d'exemples de normes de codage de la couche physique, similaires au codage Manchester pour Ethernet. Entre autres choses, ces méthodes de signalisation différencient les méthodes de communication série entre elles. Parmi les nombreuses normes de communication série, on trouve les suivantes:

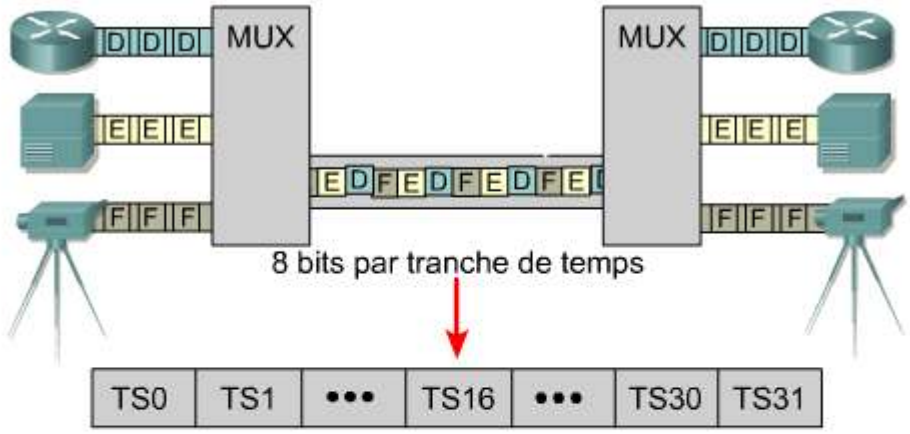
- RS-232-E
- V.35
- HSSI (High Speed Serial Interface)

3.1 Liaisons série point-à-point

3.1.2 Multiplexage temporel

Le multiplexage temporel (TDM – *Time-division multiplexing*) désigne la transmission de plusieurs sources d'informations sur un canal, ou signal, commun, puis la reconstruction des flux d'origine à l'extrémité distante.

Dans l'exemple présenté à la Figure 1, trois sources d'informations sont transportées tour à tour sur le canal de sortie. Tout d'abord, un bloc d'informations est prélevé de chaque canal d'entrée. La taille de ce bloc peut varier, mais il s'agit généralement d'un bit ou d'un octet. Selon que des bits ou des octets sont utilisés, ce type de TDM est appelé entrelacement de bits ou entrelacement d'octets.



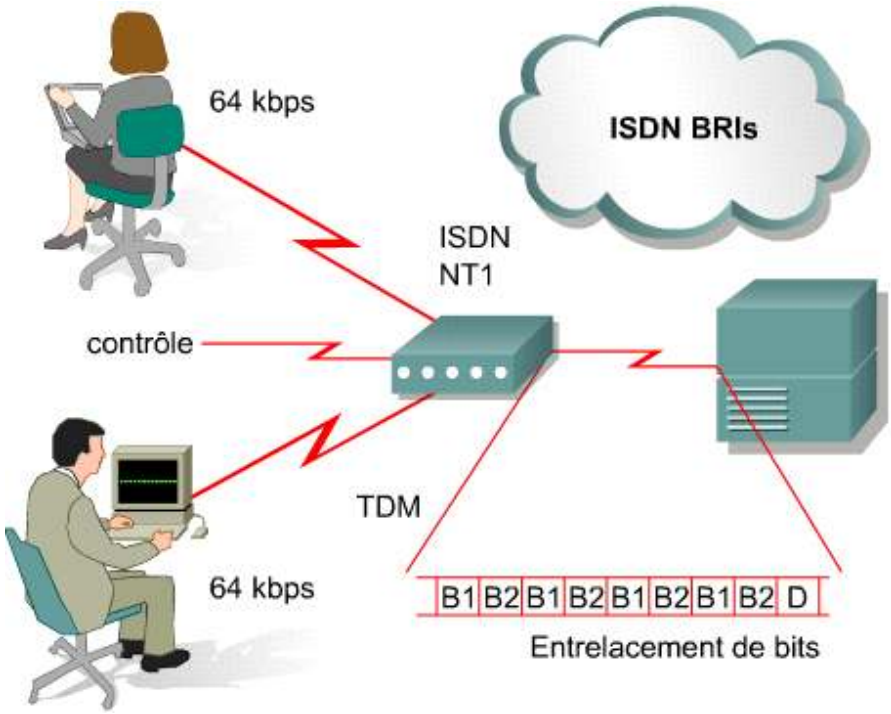
- Les " tranches de temps " sont toujours présentes même si aucune donnée n'est disponible pour l'envoi.
- La largeur de bande est allouée à l'application de façon statique.
- TDM est indépendant de tout protocole (HDLC, PPP).

Chacun des trois canaux d'entrée a sa propre capacité. Pour que le canal de sortie puisse accepter les informations provenant des trois entrées, sa capacité ne doit pas être inférieure au total de ces entrées.

Dans le TDM, l'intervalle de temps de sortie est toujours présent, que l'entrée ait ou non des informations à transmettre. La sortie TDM peut être comparée à un train avec 32 wagons. Chacun d'entre eux appartient à une société de routage différente et chaque jour, le train part avec ses 32 wagons. Si l'une des sociétés a des produits à expédier, le wagon est chargé. Si la société n'a rien à envoyer, le wagon reste vide, mais fait toujours partie du train.

TDM agit au niveau de la couche physique et ignore la nature des informations multiplexées vers le canal de sortie. Le TDM est indépendant du protocole de couche 2 qui a été utilisé par les canaux d'entrée.

Le réseau RNIS (*Réseau numérique à intégration de services*) est un exemple de TDM. RNIS accès de base (BRI) comporte trois canaux, à savoir deux canaux B à 64 kbits/s (B1 et B2) et un canal D à 16 kbits/s. Le TDM comporte neuf intervalles de temps, qui se répètent. Dans les autres pays du monde, l'unité de terminaison de réseau (NTU) est fournie et gérée par l'opérateur téléphonique. 2



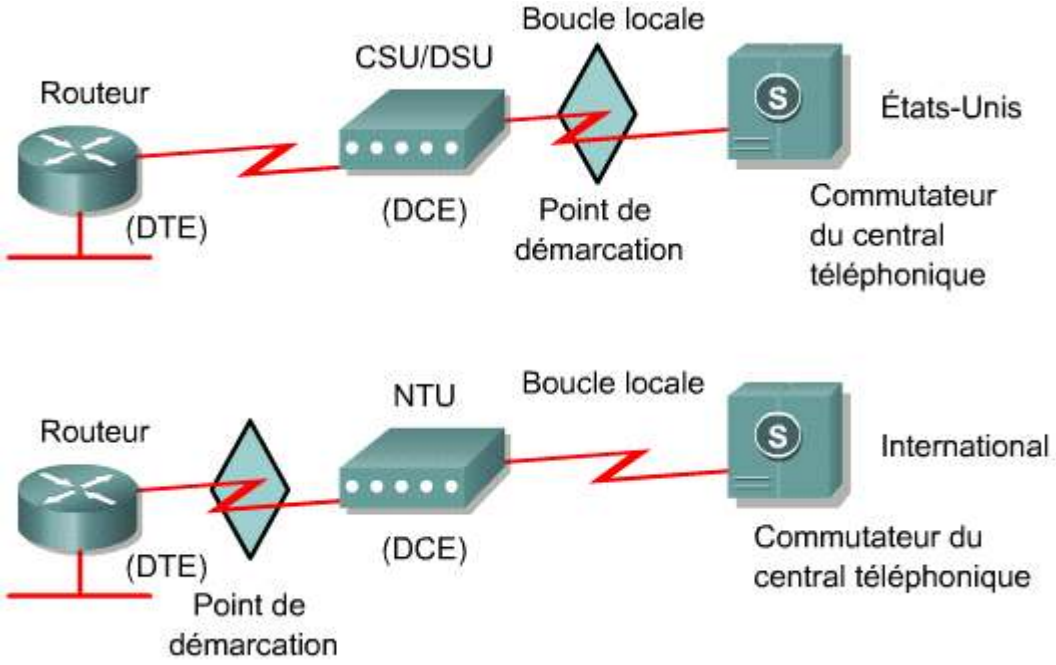
Ceci permet à ce dernier de gérer et de dépanner la boucle locale de façon réactive, car le point de démarcation se situe après la NTU. Le client connecte un CPE (*customer premises equipment* – équipement placé chez le client par l'opérateur), tel qu'un routeur ou un matériel d'accès frame relay, dans la NTU par l'intermédiaire d'une interface série V.35 ou RS-232.

3.1 Liaisons série point-à-point

3.1.3 Point de démarcation

Le point de démarcation de service est le point du réseau où la responsabilité du fournisseur d'accès, ou opérateur téléphonique, prend fin. Aux États-Unis, un opérateur fournit la boucle locale dans les locaux du client et le client fournit l'équipement actif, tel que l'unité CSU/DSU (*channel service unit/data service unit*) sur laquelle la boucle locale se termine. Cette terminaison est souvent située dans une armoire de télécommunications, le client étant responsable de la maintenance, du remplacement ou de la réparation de l'équipement.

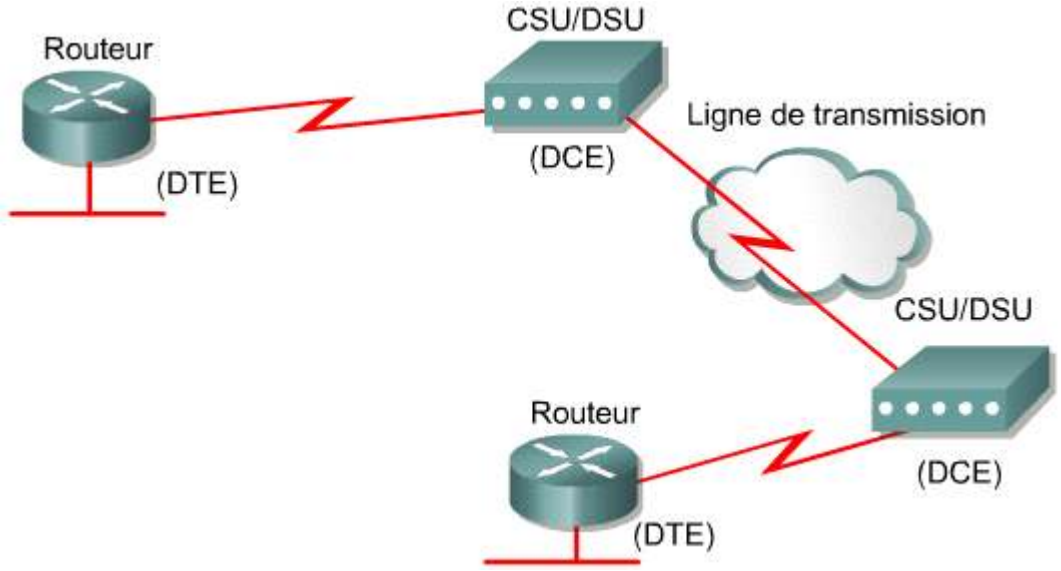
Dans les autres pays du monde, l'unité de terminaison de réseau (NTU) est fournie et gérée par l'opérateur téléphonique. Ceci permet à ce dernier de gérer et de dépanner la boucle locale de façon réactive, car le point de démarcation se situe après la NTU. Le client connecte un CPE (*customer premises equipment* – équipement placé chez le client par l'opérateur), tel qu'un routeur ou un matériel d'accès frame relay, dans la NTU par l'intermédiaire d'une interface série V.35 ou RS-232. 1



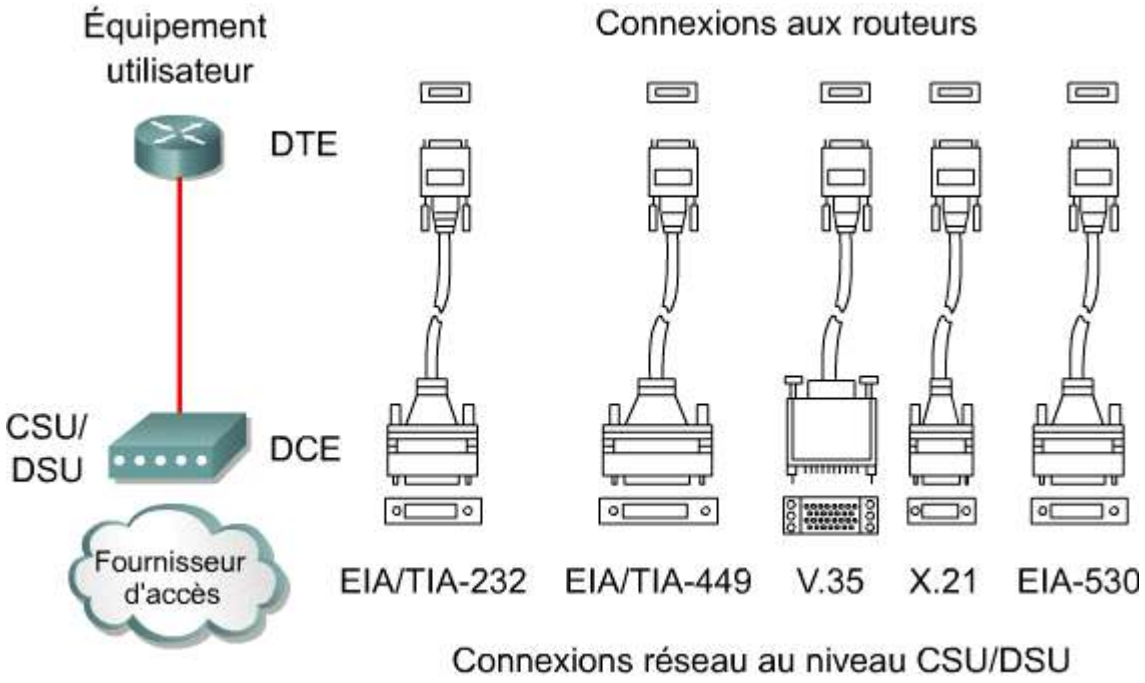
3.1 Liaisons série point-à-point

3.1.4 ETCD/ETTD

Une connexion série comporte un équipement terminal de traitement de données (ETTD) à une extrémité de la connexion et un équipement de communication de données (ETCD) à l'autre extrémité. La connexion entre les deux ETCD est le réseau de transmission du fournisseur du réseau WAN. Le CPE, généralement un routeur, constitue l'ETTD. Il peut également s'agir d'un terminal, d'un ordinateur, d'une imprimante ou d'un télécopieur. L'ETCD, généralement un modem ou une unité CSU/DSU, est l'équipement servant à convertir les données utilisateur de l'ETTD en une forme compatible avec la liaison de transmission du fournisseur d'accès au WAN. Le signal est reçu par l'ETCD distant, qui le décode en une séquence de bits. Cette séquence est ensuite signalée à l'ETTD. 1



De nombreuses normes ont été développées pour permettre aux ETTD de communiquer avec les ETCD. L'EIA (*Electronics Industry Association*) et l'ITU-T (*International Telecommunication Union Telecommunications Standardization Sector*) ont été les plus actifs dans le développement de ces normes. 2



L'ITU-T désigne l'ETCD comme l'équipement terminal de circuit de données. L'EIA désigne l'ETCD comme l'équipement de communication de données (DCE – data communication equipment).

L'interface ETCD/ETTD d'une norme particulière définit les spécifications ci-dessous:

- **Mécanique/physique** – Nombre de broches et type de connecteur
- **Électrique** – Définit les niveaux de tension pour 0 et 1
- **Fonctionnelle** – Spécifie les fonctions exécutées en attribuant des significations à chacune des lignes de signalement de l'interface
- **Procédurale** – Spécifie la séquence d'événements pour la transmission des données

Si deux ETTD doivent être interconnectés, comme deux ordinateurs ou deux routeurs dans le TP, un câble spécial, appelé «null-modem», s'avère nécessaire pour se dispenser d'un ETCD. Pour les connexions synchrones, pour lesquelles un signal d'horloge est nécessaire, un équipement externe ou l'un des ETTD doit générer ce signal d'horloge.

Le port série synchrone d'un routeur est configuré comme ETTD ou ETCD en fonction du câble qui y est relié, commandé comme ETTD ou ETCD pour correspondre à la configuration du routeur. Si le port est configuré en ETTD, le réglage par défaut, une horloge externe est requise au niveau de l'unité CSU/DSU ou d'un autre équipement ETCD.

Le câble de connexion de l'ETTD à l'ETCD est un câble de transmission série blindé. L'extrémité routeur du câble de transition série blindé peut être un connecteur DB-60, qui se branche dans le port DB-60 d'une carte d'interface WAN série. L'autre extrémité du câble peut ensuite recevoir le connecteur approprié à la norme utilisée. Le fournisseur du WAN ou l'unité CSU/DSU dicte généralement le type de câble requis. Les équipements Cisco prennent en charge les normes série EIA/TIA-232, EIA/TIA-449, V.35, X.21 et EIA/TIA-530.

Pour prendre en charge des densités plus élevées avec un encombrement réduit, Cisco a créé le câble série intelligent (Smart Serial cable). L'extrémité routeur du câble série intelligent est un connecteur 26 broches considérablement plus compact que le connecteur DB-60.

Activité de média interactive

Agrandissement: Câble ETCD/ETTD

Dans cette vue agrandie, l'étudiant peut voir un câble ETCD et ETTD.

3.1 Liaisons série point-à-point

3.1.5 Encapsulation HDLC

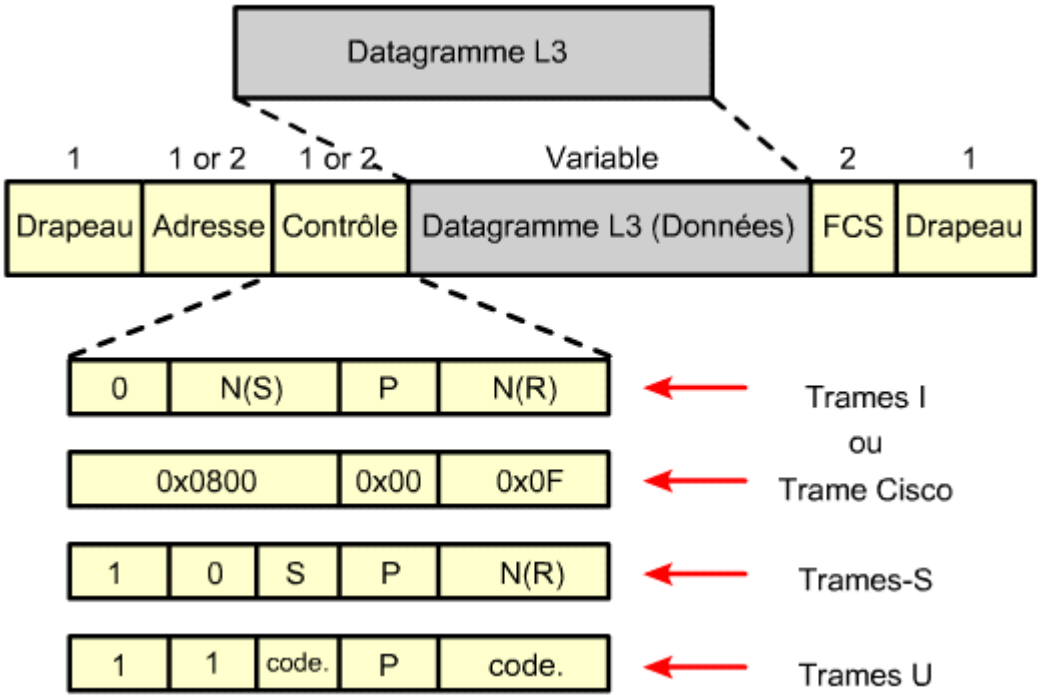
À l'origine, les communications série étaient fondées sur des protocoles orientés caractères. Les protocoles orientés Bits étaient plus efficaces, mais étaient également propriétaires. En 1979, l'ISO accepta HDLC, qui est un protocole de couche liaison de données, comme une norme orientée bits qui encapsule les données sur des liaisons série synchrones. Cette normalisation a mené d'autres comités à adopter et à développer le protocole. Depuis 1981, ITU-T a développé une série de protocoles dérivés de HDLC. Les exemples suivants de protocoles dérivés sont appelés des protocoles d'accès de liaison :

- Procédure d'accès en mode équilibré LAPB (*Link Access Procedure*), for X.25
- Protocole de liaison LAPD (*Link Access Procedure – D channel*) pour RNIS
- Procédure de liaison pour modems LAPM (Link Access Procedure for Modems) et PPP pour les modems
- Procédure de liaison pour Frame Relay LAPF (*Link Access Procedure for Frame Relay*) pour Frame Relay

HDLC utilise une transmission série synchrone offrant des communications sans erreurs entre deux points. HDLC définit une structure de tramage de couche 2 permettant un contrôle de flux et d'erreurs au moyen d'accusés de réception et d'un schéma de fenêtrage. Chaque trame présente le même format, qu'il s'agisse d'une trame de données ou d'une trame de contrôle.

Le protocole HDLC ne prend pas en charge de façon inhérente plusieurs protocoles sur une seule liaison, car il n'a aucun moyen d'indiquer le protocole transporté. Cisco offre une version propriétaire de HDLC. La trame HDLC de Cisco utilise un champ « type » propriétaire servant de champ de protocole. Ce champ permet à plusieurs protocoles de couche réseau de partager la même liaison série. HDLC constitue le protocole de couche 2 par défaut pour les interfaces série des routeurs Cisco.

HDLC définit les trois types de trame ci-dessous, chacune présentant un format de champ de contrôle différent: 1



- **Les trames d'information (Trames I)** – Transportent les données à transmettre pour la station. Elles offrent un contrôle de flux et d'erreurs supplémentaire et les données peuvent être superposées sur une trame d'informations.
- **Les trames de supervision (Trames S)** – Fournissent des mécanismes de requête/réponse quand la superposition n'est pas utilisée.
- **Trames non-numérotées (Trames U)** – Fournissent des fonctions supplémentaires de contrôle des liaisons, telles que la configuration de connexion. Le champ de code définit le type de trame U.

Les un ou deux premiers bits du champ de contrôle servent à identifier le type de trame. Dans le champ de contrôle d'une trame d'information (I), le numéro de séquence d'envoi désigne le numéro de la trame suivante à envoyer. Le numéro de séquence de réception fournit le numéro de la trame suivante à recevoir. L'émetteur et le récepteur s'occupent de la maintenance des numéros de séquence d'envoi et de réception.

3.1 Liaisons série point-à-point

3.1.6 Configuration de l'encapsulation HDLC

Cisco HDLC est la méthode d'encapsulation par défaut utilisée par les équipements Cisco sur des lignes série synchrones. Si l'interface série est configurée avec un autre protocole d'encapsulation et que l'encapsulation doit être replacée en HDLC, accédez au mode de configuration de l'interface série. Entrez ensuite la commande **`encapsulation hdlc`** pour spécifier le protocole d'encapsulation de l'interface. 1

```
Router(config-if)#encapsulation hdlc
```

- Activez l'encapsulation HDLC
- HDLC est l'encapsulation par défaut sur les interfaces série synchrones

Cisco HDLC est un protocole point-à-point pouvant être utilisé sur des lignes louées entre deux équipements Cisco. Pour communiquer avec un équipement d'une autre marque que Cisco, le PPP synchrone constitue une option plus viable.

3.1 Liaisons série point-à-point

3.1.7 Dépannage d'une interface série

Les résultats de la commande **`show interfaces serial`** présentent des informations spécifiques aux interfaces série. Quand HDLC est configuré «Encapsulation HDLC» doit apparaître dans les résultats. 1

```
Router#show interfaces s0/0
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.108.156.98, subnet mask is
255.255.255.240
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set
(10 sec)
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 5762 drops; input queue 0/75, 301
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface
resets
     0 output buffer failures, 0 output buffers swapped
out
     482 carrier transitions
        DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Quand PPP est configuré, «Encapsulation PPP» doit apparaître dans les résultats.

```
Router#show interfaces serial s0/0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10
sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface
resets
     0 output buffer failures, 0 output buffers swapped
out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Cinq états de problème possibles peuvent être identifiés sur la ligne d'état de l'interface affichée par **`show interfaces serial`**: 3

- L'interface série x est désactivée et le protocole de ligne est désactivé (Serial x is down, line protocol is down)
- L'interface série x est activée et le protocole de ligne est désactivé
- L'interface série x est activée et le protocole de ligne est activé (en boucle)
- L'interface série x est activée et le protocole de ligne désactivé
- L'interface série x est désactivée pour des raisons d'administration (administratively down) et le protocole de ligne est désactivé

Ligne d'état	Condition possible	Solution du problème
L'interface série x est activée et le protocole de ligne activé	Il s'agit de la condition de ligne d'état correcte.	Aucune action n'est requise.
L'interface série x est désactivée et le protocole de ligne est désactivé	Le routeur ne capte aucun signal de CD, ce qui signifie que le CD n'est pas actif. Un problème est survenu chez le fournisseur d'accès WAN, ce qui implique que la ligne est inactive ou n'est pas connectée à une unité Le câblage est défectueux ou incorrect. Une defaillance matérielle est survenue (CSU/DSU).	1. Vérifiez les diodes électroluminescentes (LED) de l'unité CSU/DSU pour déterminer si le CD est actif, ou insérez une boîte de dérivation sur la ligne pour vérifier le signal du CD. 2. Assurez-vous que le câble et l'interface utilisés sont corrects en consultant la documentation d'installation du matériel. 3. Insérez une boîte de dérivation et vérifiez tous les câbles de contrôle. 4. Contactez le fournisseur de la ligne louée ou votre opérateur pour déterminer s'il existe un problème. 5. Changez les pièces défectueuses. 6. Si vous suspectez que le matériel du routeur est défectueux, placez la ligne série sur un autre port. Si la connexion s'établit, l'interface précédemment connectée a un problème.
L'interface série x est activée et le protocole de ligne est désactivé (mode ETTD)	Un routeur local ou distant est mal Aucun test d'activité n'est envoyé par le routeur distant. Un problème au niveau d'une ligne louée ou d'un autre service de l'opérateur est survenu, ce qui indique une ligne bruitée ou un Un problème d'horloge est survenu sur le câble, ce qui signifie que l'horloge de transmission série externe (SCTE) n'est pas configurée sur l'unité CSU/DSU. La SCTE est conçue pour compenser le décalage de phase dans les longs câbles. Lorsque l'ETCD utilise la SCTE Une unité CSU/DSU locale ou distance est Le matériel d'un routeur local ou distant est tombé en panne.	1. Mettez le modem ou l'unité CSU/DSU en mode bouclé et utilisez la commande **`show interfaces serial`** pour déterminer si le protocole de ligne s'active. Si le protocole de ligne s'active, il est probable que le fournisseur d'accès WAN ou qu'un routeur distant 2. Si le problème semble provenir de l'extrémité distante, répétez l'étape 1 sur le modem distant ou l'unité CSU ou DSU. 3. Vérifiez tout le câblage. Assurez-vous que le câble est connecté à l'interface appropriée, à l'unité CSU/DSU appropriée et au point de terminaison approprié sur le réseau du fournisseur d'accès WAN. Utilisez la commande show controllers exec pour déterminer quel câble est connecté à quelle 4. Activez la commande de débogage **`serial interface exec`** . 5. Si le protocole de ligne ne s'active pas en mode bouclé local et si la commande **`debug serial interface`** indique que le compteur de test d'activité ne s'incrémente pas, il est probable qu'un problème soit survenu au niveau du matériel d'un routeur. Changez le matériel 6. Si le protocole de ligne s'active et que le compteur de test d'activité s'incrémente, le problème ne provient pas du routeur local. 7. Si vous suspectez que le matériel du routeur est défectueux, placez la ligne série sur un port inutilisé. Si la connexion s'établit, l'interface précédemment connectée a un problème.

L'interface série x est activée et le protocole de ligne est désactivé (mode ETCD)	La commande de configuration de fréquence d'horloge de l'interface est absente. L'équipement ETTD ne prend pas en charge ou n'est pas configuré pour le mode SCTE (horloge terminal). L'unité CSU ou DSU distante est tombée en panne.	1. Ajoutez la commande de configuration de fréquence d'horloge à l'interface série. Syntaxe : **clockrate** *bps* Description de la syntaxe : bits/s - Taux d'horloge souhaité en bits par seconde : 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000 2. Si le problème semble provenir de l'extrémité distante, répétez l'étape 1 sur le modem distant ou l'unité CSU ou DSU. 3. Vérifiez que le câble approprié est utilisé. 4. Si le protocole de ligne ne fonctionne toujours pas, il existe vraisemblablement un problème de défaillance matérielle ou de câblage. Insérez une boîte de dérivation et observez les câbles.
L'interface série x est activée et le protocole de ligne est activé (en boucle)	Il y a une boucle dans le circuit. Le numéro de séquence du paquet de test d'activité adopte un numéro aléatoire à la détection initiale d'une boucle. Si le même numéro aléatoire est renvoyé sur la liaison, une boucle est présente.	1. Utilisez, en mode privilégié, la commande **show running-config** pour voir s'il existe des entrées de commande de configuration 2. Si vous trouvez une entrée de commande de configuration **l loopback** , lancez la commande **l no loopback** pour éliminer la boucle. 3. Si il n'y a pas de conflit d'interfaces d'essai en mode bouclé, inspectez physiquement l'unité CSU/DSU afin de déterminer si elle peut être mise manuellement en mode d'essai. Si c'est le cas, désactivez le bouclage manuel. 4. Après avoir désactivé le mode d'essai sur l'unité CSU/DSU, réinitialisez-la et inspectez le statut de la ligne. Si le protocole de ligne s'active, aucune autre action n'est requise. 5. Si l'unité CSU/DSU n'est pas configurable manuellement, contactez le fournisseur de la ligne louée ou l'opérateur pour obtenir de l'assistance
L'interface série x est activée et le protocole de ligne est désactivé (disabled)	Un taux d'erreur élevé est survenu du fait d'un problème au niveau du fournisseur d'accès WAN. Un problème est survenu au niveau du matériel d'une unité CSU ou DSU. Le matériel du routeur (interface) est hors service.	1. Pour dépanner la ligne, utilisez un analyseur série et une boîte de dérivation. Recherchez les signaux CTS et DSR changeants. 2. Bouclez l'unité CSU/DSU (boucle DTE). Si le problème persiste, un problème matériel est vraisemblablement en cause. Si le problème ne continue pas, il est probable que le problème se situe au niveau du fournisseur d'accès WAN. 3. Changez le matériel défectueux (CSU, DSU, commutateur, routeur local ou distant).

L'interface série x est désactivée pour des raisons d'administration (administratively down) et le protocole de ligne est désactivé	La configuration du routeur inclut la commande de configuration de désactivation de l'interface. Il existe une adresse IP dupliquée.	1. Vérifiez la configuration du routeur pour la commande **shutdown**. 2. Utilisez la commande **no shutdown interface** pour supprimer la commande **shutdown**. 3. Assurez-vous qu'il n'existe aucune adresse IP identique au moyen de la commande en mode privilégié **show running-config** ou de la commande **show interfaces exec** . 4. Si des adresses sont dupliquées, changez l'une des adresses IP pour résoudre le conflit.

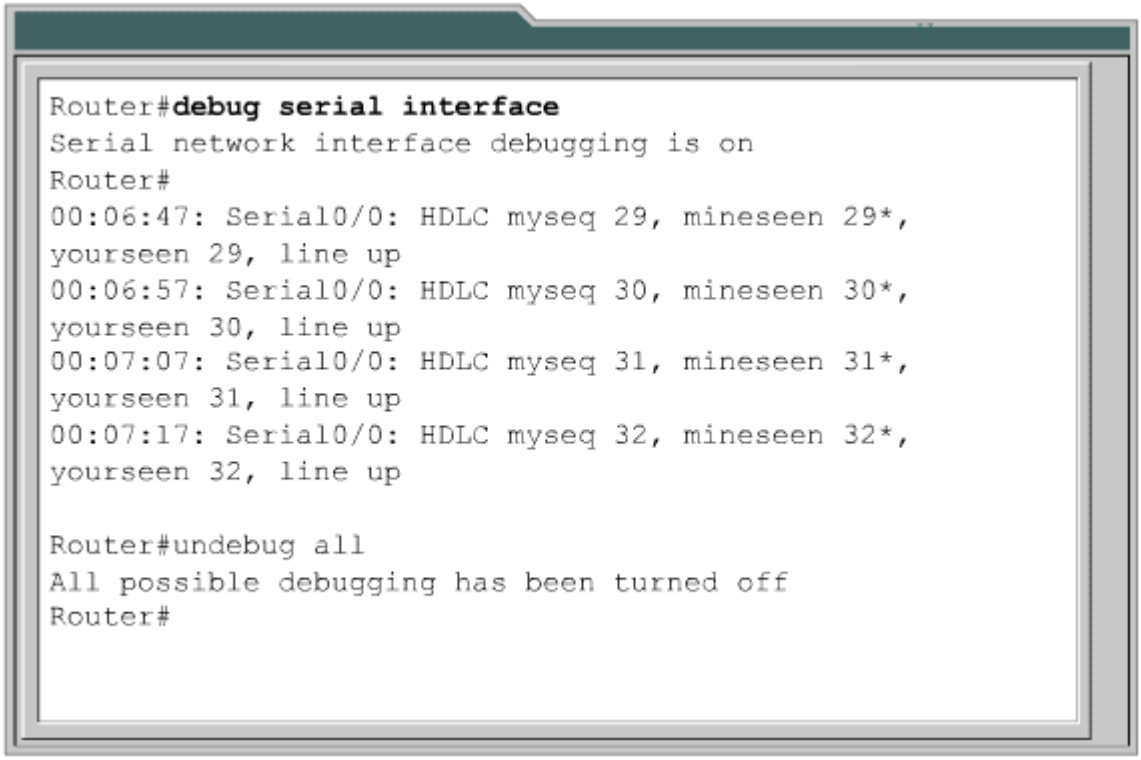
La commande **show controllers** est un autre outil de diagnostic important pour le dépannage des lignes série. Les résultats renvoyés par **show controllers** indiquent l'état des canaux de l'interface et signalent la présence ou l'absence d'un câble. À la figure 4, un câble DTE V.35 est relié à l'interface série 0/0. La syntaxe de la commande est variable, en fonction de la plate-forme. Pour les interfaces série des routeurs de la série Cisco 7000, utilisez la commande **show controllers cbus**.

```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x81414E2C, driver data structure at 0x8141753C
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific
[PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status
[SCCS]=0x06
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
```

Si la sortie de l'interface électrique apparaît comme UNKNOWN, au lieu de V.35, EIA/TIA-449, ou un autre type d'interface électrique, c'est probablement un câble mal connecté qui est à l'origine du problème. Il est également possible que le câblage interne de la carte présente un problème. Si l'interface électrique est inconnue, l'écran correspondant à la commande **show interfaces serial** <X> montre que l'interface et le protocole de ligne sont désactivés.

Des commandes de débogage, utiles pour résoudre les problèmes d''interface série et de WAN, sont présentées ci-dessous:

- **debug serial interface** – Vérifie si les paquets de veille HDLC s'incrémentent. S'ils ne s'incrémentent pas, il existe probablement un problème de synchronisation sur la carte d'interface ou le réseau. 5


Router#debug serial interface
Serial network interface debugging is on
Router#
00:06:47: Serial0/0: HDLC myseq 29, mineseen 29*,
yourseen 29, line up
00:06:57: Serial0/0: HDLC myseq 30, mineseen 30*,
yourseen 30, line up
00:07:07: Serial0/0: HDLC myseq 31, mineseen 31*,
yourseen 31, line up
00:07:17: Serial0/0: HDLC myseq 32, mineseen 32*,
yourseen 32, line up
Router#undebug all
All possible debugging has been turned off
Router#

- **debug arp** – Indique si le routeur envoie ou reçoit des informations relatives aux routeurs (avec des paquets ARP) de l'autre côté du nuage de réseau WAN. Utilisez cette commande quand certains nœuds d'un réseau TCP/IP répondent, mais d'autres non.
- **debug frame-relay lmi** – Récupère des informations sur l'interface LMI (Local Management Interface), afin de déterminer si un commutateur Frame Relay et un routeur envoient et reçoivent des paquets LMI.
- **debug frame-relay events** – Détermine si des échanges se produisent entre un routeur et un commutateur Frame Relay.
- **debug ppp negotiation** – Montre les paquets PPP (*Point-to-Point Protocol*) transmis au démarrage de PPP, au moment où les options PPP sont négociées.
- **debug ppp packet** – Montre les paquets PPP envoyés et reçus. Cette commande affiche les transferts de paquets à bas niveau.
- **debug ppp** – Montre les erreurs PPP, telles que les trames illégales ou déformées, associées à la négociation et à l'utilisation de la connexion PPP.
- **debug ppp authentication** – Montre les échanges de paquets PPP CHAP (*Challenge Handshake Authentication Protocol*) et PAP (*Password Authentication Protocol*).

ATTENTION:

Les résultats de débogage reçoivent une haute priorité dans le processus du CPU et peuvent rendre le système inutilisable. C'est pourquoi les commandes de débogage doivent seulement être utilisées pour résoudre des problèmes spécifiques, ou au cours de sessions de dépannage avec le personnel d'assistance technique de Cisco. Il est recommandé d'utiliser les commandes de déboguage pendant les périodes creuses du réseau et lorsque le nombre d'utilisateurs connectés est le plus bas possible. En effet, un débogage pendant ces périodes réduit les risques que la surcharge due au traitement de ces commandes ait des répercussions sur le système.

Activité de TP

Exercice: Dépannage d'une interface série

Au cours de ce TP, les étudiants vont configurer une interface série sur les routeurs London et Paris.

Activité de TP

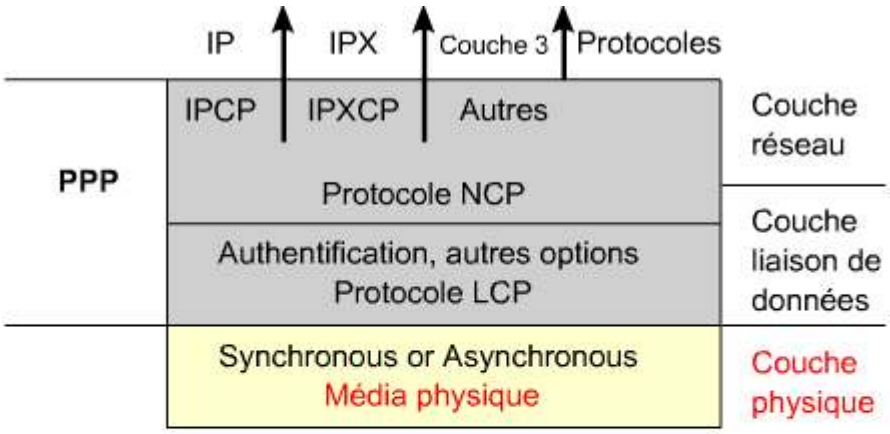
Activité en ligne: Dépannage d'une interface série

Au cours de ce TP, les étudiants vont configurer une interface série sur les routeurs London et Paris.

3.2 Authentification PPP

3.2.1 Architecture multicouche PPP

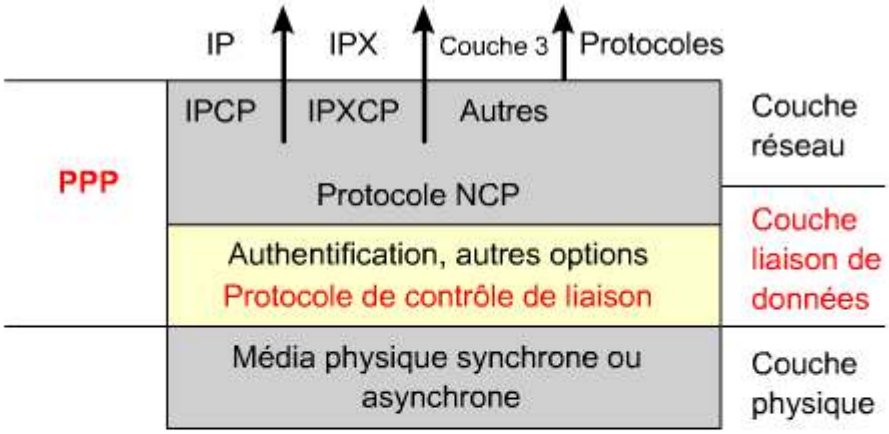
PPP utilise une architecture multicouche. Une architecture multicouche est un modèle, une conception ou un plan d'action logique facilitant la communication entre des couches interconnectées. Le modèle OSI (Open System Interconnection) est l'architecture multicouche utilisée dans les réseaux. PPP fournit une méthode d'encapsulation des datagrammes multiprotocoles sur une liaison point-à-point et utilise la couche de liaison de données pour tester la connexion. Par conséquent, PPP est constitué de deux sous-protocoles: 1



Avec ses fonctions de bas niveau, le protocole PPP utilise les éléments suivants :

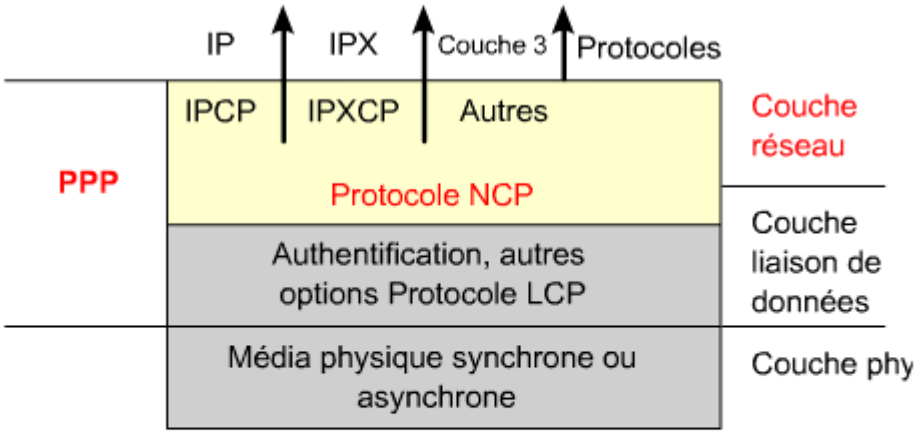
- Média physique synchrone
- Média physique asynchrone, tel que ceux utilisés par le service téléphonique de base pour les connexions commutées par modem.

- **Le protocole de contrôle de liaison (LCP pour Link Control Protocol)** – Utilisé pour établir la liaison point-à-point. 2



- PPP offre de nombreux services permettant de contrôler la mise en place d'une liaison de données.
- Ces services sont des options de LCP et sont principalement des trames de négociation et de vérification destinées à mettre en oeuvre les contrôles point à point qu'un administrateur spécifie pour l'appel.

- **Le protocole de contrôle réseau (NCP pour Network Control Protocol)** – Utilisé pour configurer les divers protocoles de couche réseau. 3



- Avec ses fonctions de haut niveau, le protocole PPP transporte des paquets de plusieurs protocoles de couche réseau grâce aux protocoles NCP.
- Il s'agit de champs fonctionnels qui contiennent des codes standard pour indiquer le type de protocole de couche réseau qu'encapsule le protocole PPP.

PPP peut être configuré sur les types suivants d'interfaces physiques:

- Série asynchrone
- Série synchrone
- HSSI (*High Speed Serial Interface*)
- RNIS (*Réseau Numérique à Intégration de Services*)

PPP utilise le protocole de contrôle de liaison (LCP) pour négocier et configurer les options de contrôle sur la liaison de données WAN. PPP utilise le protocole de contrôle réseau (NCP) pour encapsuler et négocier des options pour plusieurs protocoles de couche réseau. Le protocole LCP est situé au-dessus de la couche physique et permet d'établir, de configurer et de tester la connexion de liaison de données.

PPP utilise également LCP pour accepter automatiquement des options de format d'encapsulation, telles que:

- **L'authentification** – Le côté appelant de la liaison doit entrer des informations permettant d'assurer que l'émetteur dispose des autorisations appropriées attribuées par l'administrateur réseau pour effectuer l'appel. Les routeurs homologues échangent des messages d'authentification. Pour l'authentification, les deux choix sont le protocole d'authentification du mot de passe (PAP pour Password Authentication Protocol) et le protocole d'authentification à échanges confirmés (CHAP pour Challenge Handshake Authentication Protocol).
- **La compression** – Les options de compression augmentent le débit effectif des connexions PPP en réduisant la quantité de données sur la trame qui doit traverser la liaison. Le protocole décompresse la trame à l'arrivée. Les deux protocoles de compression disponibles sur les routeurs Cisco sont Stacker et Predictor.
- **La détection d'erreur** – Les mécanismes de détection d'erreur de PPP permettent à un processus d'identifier les conditions d'erreur. Les options Quality et Magic Number aident à assurer que la liaison de données reste fiable et sans boucle.
- **La multiliaison** – Cisco IOS version 11.1 et ultérieures prennent en charge le PPP multiliaison. Cette autre possibilité fournit un équilibrage de la charge sur les interfaces routeur utilisées par PPP.
- **Rappel PPP** – Pour renforcer la sécurité, Cisco IOS version 11.1 offre des fonctions de rappel sur PPP. Grâce à cette option LCP un routeur Cisco peut servir de client ou de serveur de rappel. Le client effectue l'appel initial, demande à être rappelé, puis met fin à son appel initial. Le routeur de rappel répond à l'appel initial et rappelle le client en s'appuyant sur ses instructions de configuration.

LCP effectue également les opérations suivantes:

- Il gère les limites variables de taille de paquets
- Il détecte les erreurs de configuration courantes
- Il met fin à la liaison
- Il détermine si une liaison fonctionne correctement ou présente des défaillances

Avec PPP, plusieurs protocoles de couche réseau peuvent fonctionner sur la même liaison de communications. Pour chaque protocole de couche réseau utilisé, un protocole de contrôle réseau (NCP) est fourni. Par exemple, le protocole IP (Internet Protocol) utilise le protocole de contrôle IP (IPCP), et IPX (Internetwork Packet Exchange) utilise le protocole de contrôle Novell IPX (IPXCP). Les NCP incluent des champs fonctionnels qui contiennent des codes standard pour indiquer le type de protocole de couche réseau qu'encapsule le protocole PPP.

Une trame de l'interface PPP comporte les champs suivants:

- **Drapeau** – Indique le début ou la fin d'une trame et comprend la séquence binaire 01111110.
- **Adresse** – Comprend l'adresse de broadcast standard composée de la séquence binaire 11111111. Le protocole PPP n'attribue pas d'adresse de station individuelle.
- **Contrôle** –Comprend un octet composé de la séquence binaire 00000011, qui appelle la transmission des données utilisateur dans une trame non séquencée. Un service non orienté connexion semblable au contrôle de lien logique (LLC) de type 1 est fourni.
- **Protocole** – Comprend deux octets qui identifient le protocole encapsulé dans le champ de données de la trame. 4

Valeur (hex)	Nom du protocole
8021	Internet Protocol Control Protocol
8023	Protocole de contrôle de couche réseau OSI
8029	Protocole de contrôle Appletalk
802b	Protocole de contrôle IPX de Novell
c021	Protocole de contrôle de liaison
c023	Protocole d'authentification du mot de passe
c223	Protocole d'authentification à échanges confirmés

- **Données** – Comprend zéro ou plusieurs octets contenant le datagramme du protocole précisé dans le champ de protocole. La fin du champ de données est identifiée par la séquence du drapeau de fermeture qui comprend les deux octets du champ de séquence de contrôle de trame (FCS). La longueur maximale par défaut du champ de données est de 1500 octets.
- **FCS** – Normalement, 16 bits ou 2 octets faisant référence aux caractères supplémentaires ajoutés à une trame à des fins de contrôle d'erreur.

Activité de média interactive

Glisser-Positionner: Architecture multicouche PPP

À la fin de cette activité, l'étudiant sera en mesure de comprendre l'architecture multicouche PPP de base.

3.2 Authentification PPP

3.2.2 Établissement d'une session PPP

L'établissement d'une session PPP se déroule en trois phases. Ces phases sont l'établissement de la liaison, l'authentification et la phase de protocole de couche réseau. 1 Des trames LCP exécutent les tâches de chaque phase LCP. Les trois catégories de trames LCP ci-dessous sont utilisées au cours d'une session PPP:

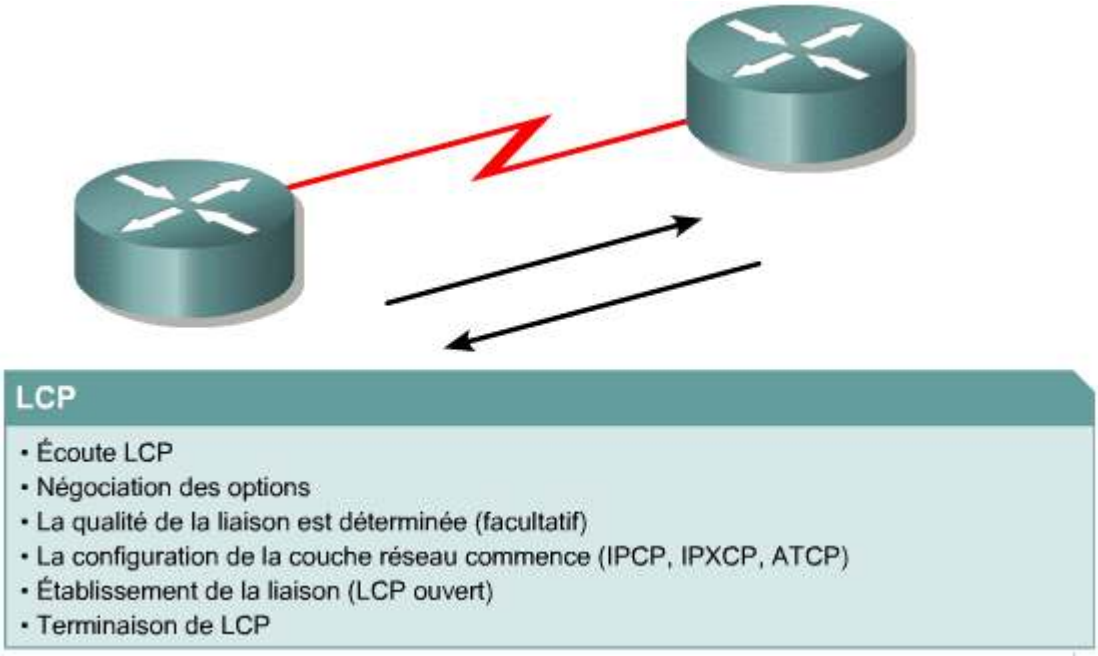
Établissement d'une session PPP

- Phase d'établissement de la liaison
- Phase d'authentification facultative
- Phase de configuration du protocole de couche réseau

- Les trames d'établissement de liaison permettent d'établir et de configurer une liaison.
- Les trames de fermeture de liaison permettent de fermer une liaison.
- Les trames de maintenance de liaison permettent de gérer et de déboguer une liaison.

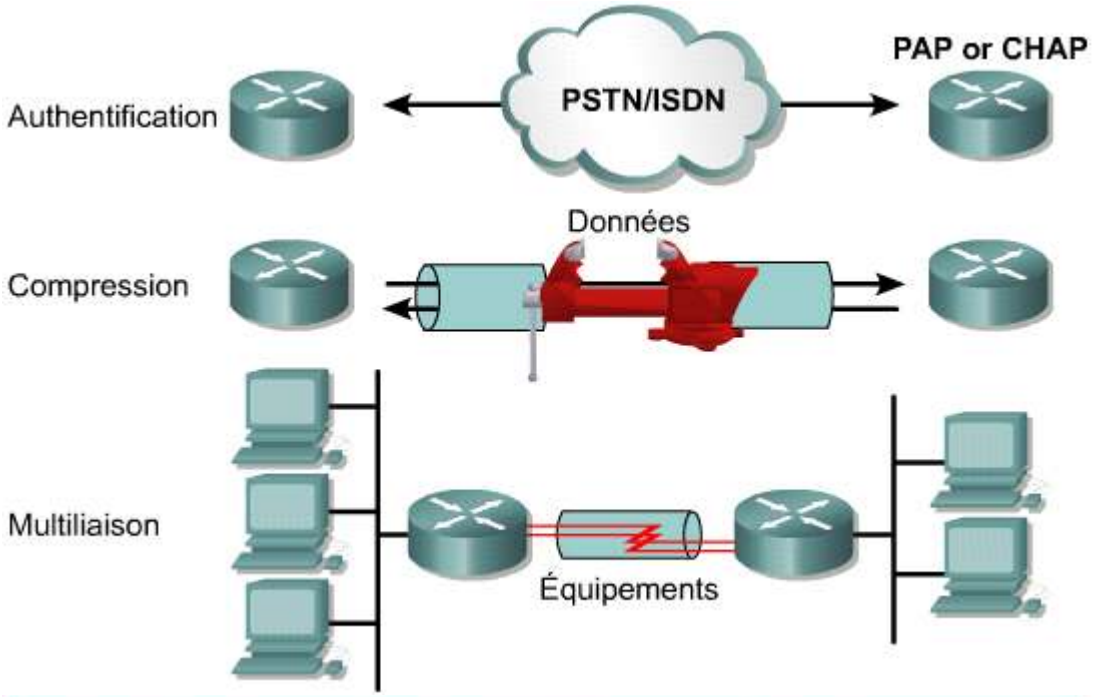
Les trois phases d'établissement d'une session PPP sont:

- **Phase d'établissement de liaison** – Au cours de cette phase, chaque équipement PPP envoie des trames LCP pour configurer et tester la liaison de données. Les trames LCP comprennent un champ d'option de configuration qui permet aux unités de négocier l'utilisation des options, telles que l'unité de transfert d'information maximale (MTU), la compression de certains champs PPP et le protocole d'authentification de la liaison. Si une option de configuration n'est pas comprise dans un paquet LCP, sa valeur par défaut est utilisée. 2


LCP
• Écoute LCP
• Négociation des options
• La qualité de la liaison est déterminée (facultatif)
• La configuration de la couche réseau commence (IPCP, IPXCP, ATCP)
• Établissement de la liaison (LCP ouvert)
• Terminaison de LCP

Avant l'échange des paquets de couche réseau, le protocole LCP doit d'abord établir la connexion et négocier les paramètres de configuration. Cette phase se termine par l'envoi et la réception d'une trame d'accusé de réception de la configuration.

- **Phase d'authentification (facultatif)** – Une fois la liaison établie et le protocole d'authentification sélectionné, l'homologue peut être authentifié. L'authentification a lieu avant le début de la phase de protocole de couche réseau. Dans le cadre de cette phase, LCP permet également d'effectuer un test facultatif de détermination de qualité de la liaison. La liaison est vérifiée afin de déterminer si sa qualité est suffisante pour activer les protocoles de couche réseau. [3] [4]



Caractéristiques	Fonctionnement	Protocole
Authentification	Demandez un mot de passe et effectuez les échanges confirmés	PAP CHAP
Compression	Compressez les données à la source et reproduisez-les à la destination	Stacker, Predictor, en-tête TCP ou MPPC
Détection d'erreurs	Surveillez les données placées sur la liaison, évitez les boucles de trame	Quality Magic Number
Multiliaison	Équilibrage de charge sur plusieurs liaisons	Protocole multiliaisons (MP)

Les routeurs Cisco qui utilisent l'encapsulation PPP peuvent inclure les options de configuration LCP présentées dans ce tableau.

- **Phase de protocole de couche réseau** – Pendant cette phase, les équipements PPP envoient des paquets NCP pour choisir et configurer un ou plusieurs protocoles de couche réseau, par exemple, IP. 5

Caractéristiques de NCP :

- Responsable de la configuration, de l'activation et de la désactivation du protocole L3
- Utilise le champ 0x8021 du protocole L2 pour identifier les données utiles comme IPCP
- Attribution d'adresses (DHCP)
- Serveurs de noms NetBIOS
- Système des noms de domaine (DNS)

- Une fois que chaque protocole de couche réseau sélectionné a été configuré, les paquets de chacun de ces protocoles sont envoyés sur la liaison. Si le protocole LCP ferme la liaison, il en informe les protocoles de couche réseau afin qu'ils prennent les mesures qui s'imposent. La commande **`show interfaces`** montre les états des trames LCP et NCP sous la configuration PPP.

La liaison PPP reste configurée pour les communications jusqu'à ce que l'un des événements ci-dessous survienne:

- Les trames LCP ou NCP ferment la liaison.
- Une horloge d'inactivité expire.
- Un utilisateur intervient.

Activité de média interactive

Glisser-Positionner: Établissement d'une session PPP

À la fin de cette activité, l'étudia connaîtra les trois étapes d'établissement d'une session PPP.

Activité de TP

Activité en ligne: show interfaces

Au cours de cette activité, l'étudiant va comprendre comment utiliser la commande **`show interfaces`** pour afficher des statistiques sur les interfaces configurées sur le routeur pour accéder au serveur.

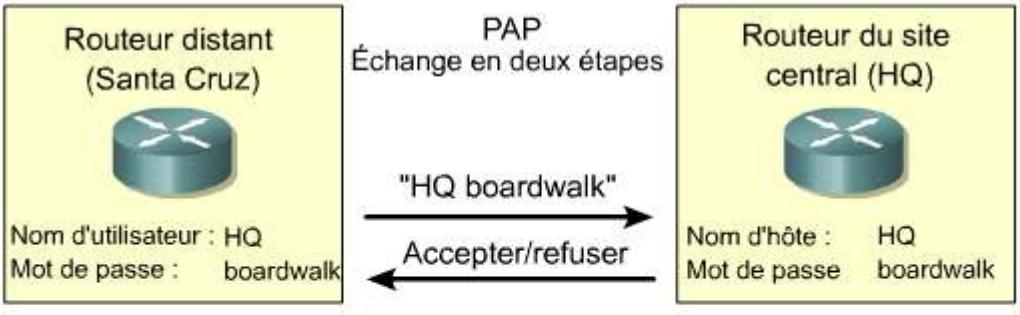
3.2 Authentification PPP

3.2.3 Protocoles d'authentification PPP

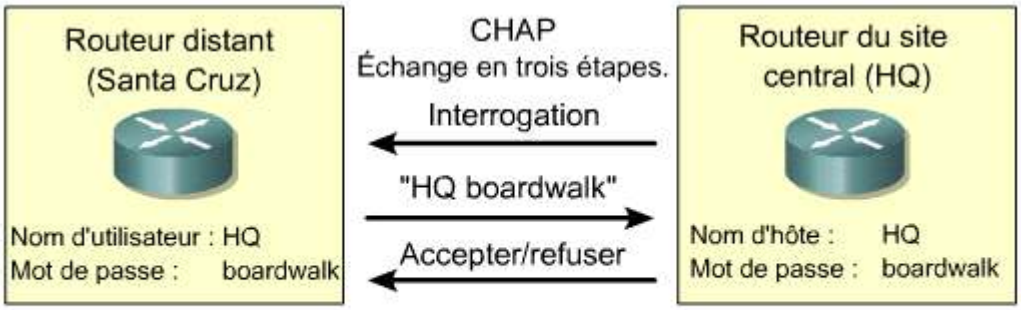
La phase d'authentification d'une session PPP est facultative. Une fois la liaison établie et le protocole d'authentification sélectionné, l'homologue peut être authentifié. L'authentification a lieu avant le début de la phase de configuration du protocole de couche réseau.

Les options d'authentification nécessitent que le côté appelant de la liaison entre des informations d'authentification. Cela aide à garantir que l'administrateur réseau a autorisé l'utilisateur à passer l'appel. Les routeurs homologues échangent des messages d'authentification.

Lors de la configuration de l'authentification PPP, l'administrateur réseau peut sélectionner le protocole d'authentification de mot de passe (PAP) ou le protocole d'authentification à échanges confirmés (CHAP). 1 2 En général, le protocole CHAP est préférable.



- Le mot de passe est envoyé en clair
- Le routeur à l'origine de la communication contrôle les tentatives

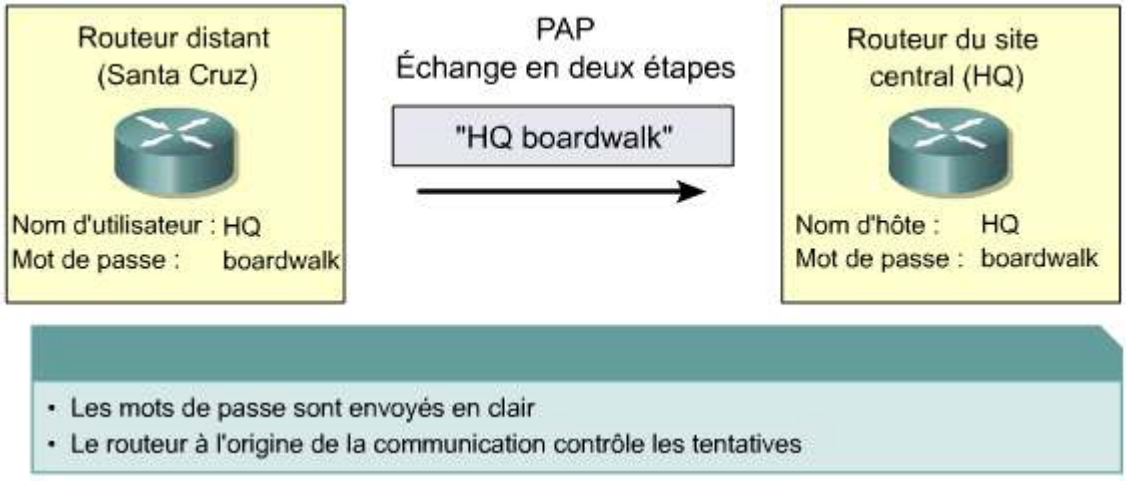


Utilise un mot de passe secret connu seulement de l'hôte d'authentification et de l'homologue.

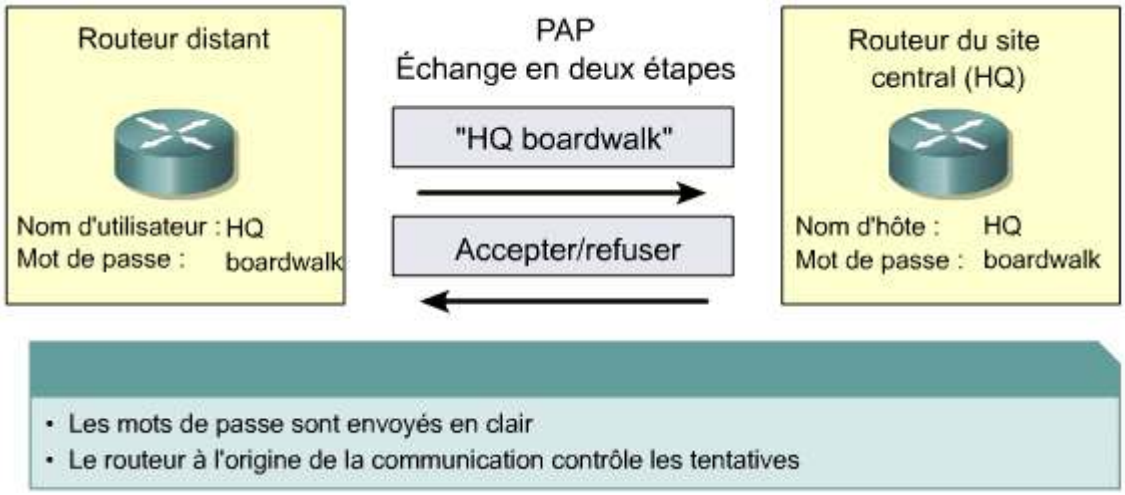
3.2 Authentification PPP

3.2.4 Protocole d'authentification du mot de passe (PAP)

Le protocole PAP procure une méthode simple permettant à un nœud distant d'établir son identité à l'aide d'un échange en deux étapes. 1


Routeur distant
(Santa Cruz)
Nom d'utilisateur : HQ
Mot de passe : boardwalk
PAP
Échange en deux étapes
"HQ boardwalk"
Routeur du site
central (HQ)
Nom d'hôte : HQ
Mot de passe : boardwalk
• Les mots de passe sont envoyés en clair
• Le routeur à l'origine de la communication contrôle les tentatives

Une fois la phase d'établissement de la liaison PPP terminée, la combinaison nom d'utilisateur/mot de passe est envoyée de façon répétée par le nœud distant sur la liaison, jusqu'à ce que l'authentification soit confirmée ou que la connexion soit interrompue. 2

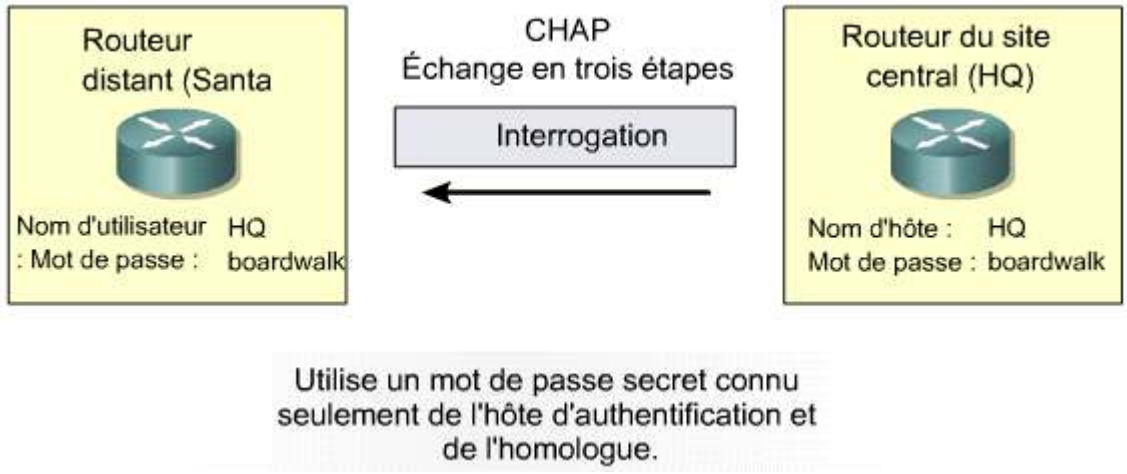

Routeur distant
Nom d'utilisateur : HQ
Mot de passe : boardwalk
PAP
Échange en deux étapes
"HQ boardwalk"
Accepter/refuser
Routeur du site
central (HQ)
Nom d'hôte : HQ
Mot de passe : boardwalk
• Les mots de passe sont envoyés en clair
• Le routeur à l'origine de la communication contrôle les tentatives

Le protocole PAP n'est pas un protocole d'authentification très efficace. En effet, les mots de passe sont transmis en clair sur la liaison et il n'offre aucune protection contre la lecture répétée des informations ou les attaques répétées par essais et erreurs. Le nœud distant contrôle la fréquence et la durée des tentatives de connexion.

3.2.5 Protocole d'authentification à échanges confirmés (CHAP)

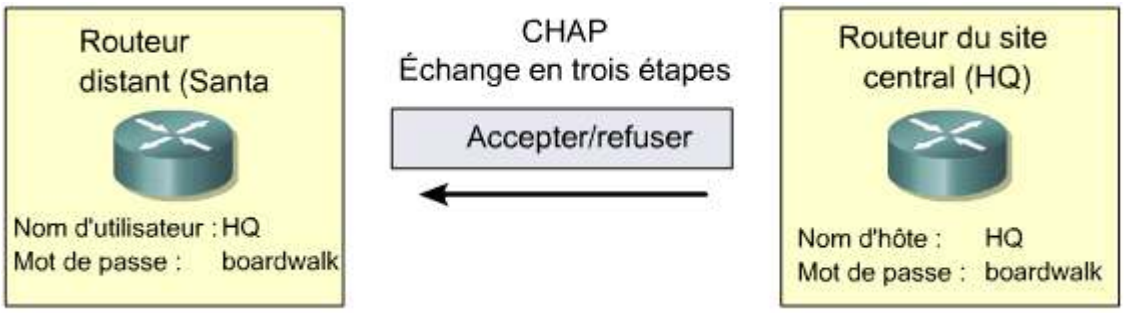
CHAP s'utilise au démarrage d'une liaison et vérifie régulièrement l'identité du nœud distant au moyen d'un échange en trois étapes. CHAP s'effectue à l'établissement initial de la liaison et se répète pendant la durée de cette liaison.

Une fois la phase d'établissement de la liaison PPP terminée, le routeur local envoie un message de demande de confirmation au nœud distant. 1



Le nœud distant répond par une valeur calculée au moyen d'une fonction de hachage unidirectionnelle, généralement l'algorithme MD5 (Message Digest 5). Cette réponse est fondée sur le mot de passe et le message de demande de confirmation. 2

Le routeur local compare la réponse à son propre calcul de la valeur hachée attendue. Si les valeurs concordent, l'authentification est acceptée ; sinon, la connexion prend fin immédiatement. 3



Le protocole CHAP protège contre les attaques de lecture répétée des informations passant par le modem en utilisant une valeur de confirmation variable, unique et imprévisible. Comme la demande de confirmation est unique et aléatoire, la valeur hachée obtenue est également unique et aléatoire. Les demandes de confirmation répétées visent à limiter la durée d'exposition à toute attaque. Le routeur local ou un serveur d'authentification externe contrôle la fréquence et la durée des demandes de confirmation.

Activité de TP

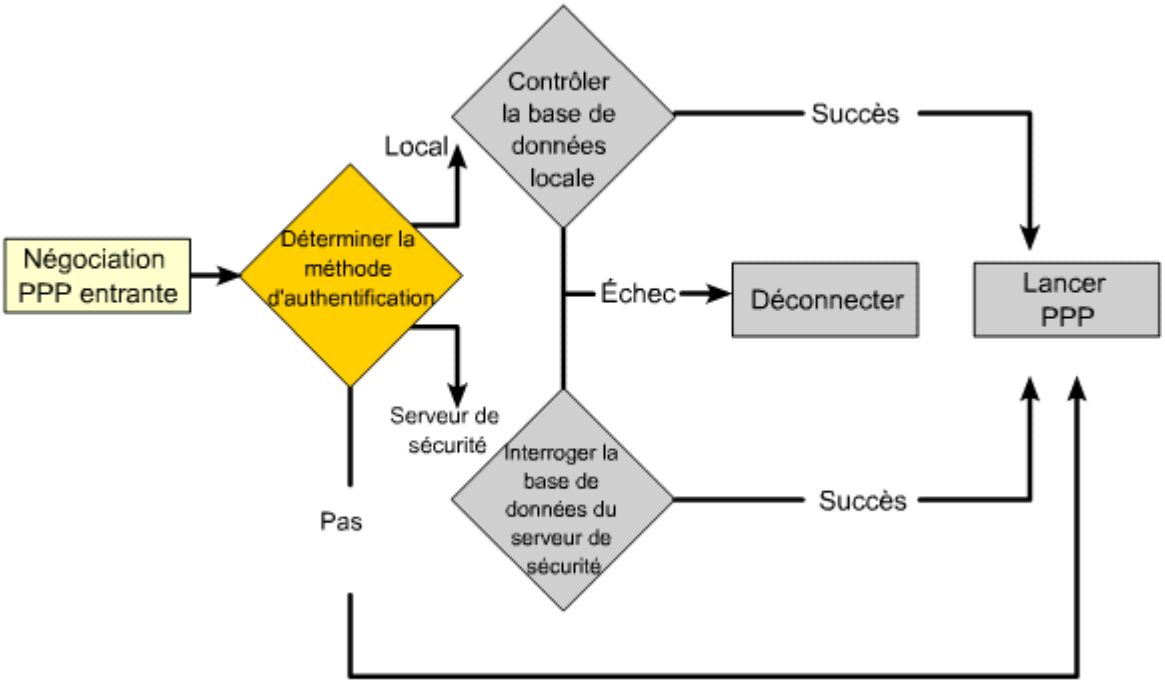
Activité en ligne: ppp chap hostname nom d'hôte

Au cours de cette activité, l'étudiant va démontrer comment utiliser la commande **`ppp chap hostname nom d'hôte`** pour créer un groupe de routeurs à accès commuté.

3.2 Authentification PPP

3.2.6 Processus d'authentification et d'encapsulation PPP

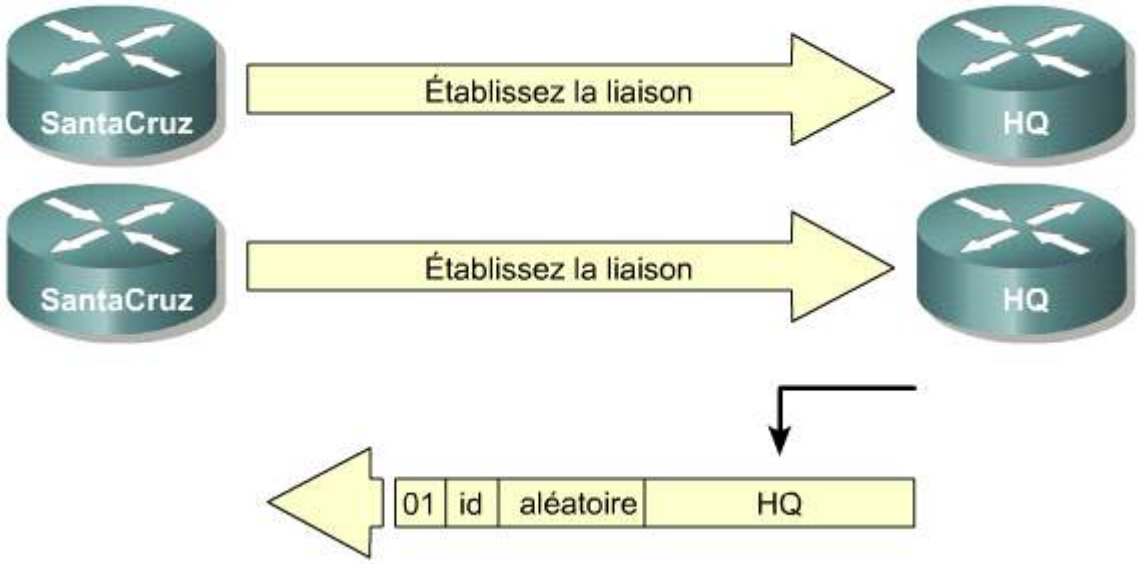
Quand la commande **`encapsulation ppp`** est utilisée, il est possible d'ajouter l'authentification PAP ou CHAP de façon facultative. Si aucune authentification n'est spécifiée, la session PPP commence immédiatement. Si une authentification est nécessaire, le processus effectue les étapes suivantes: 1

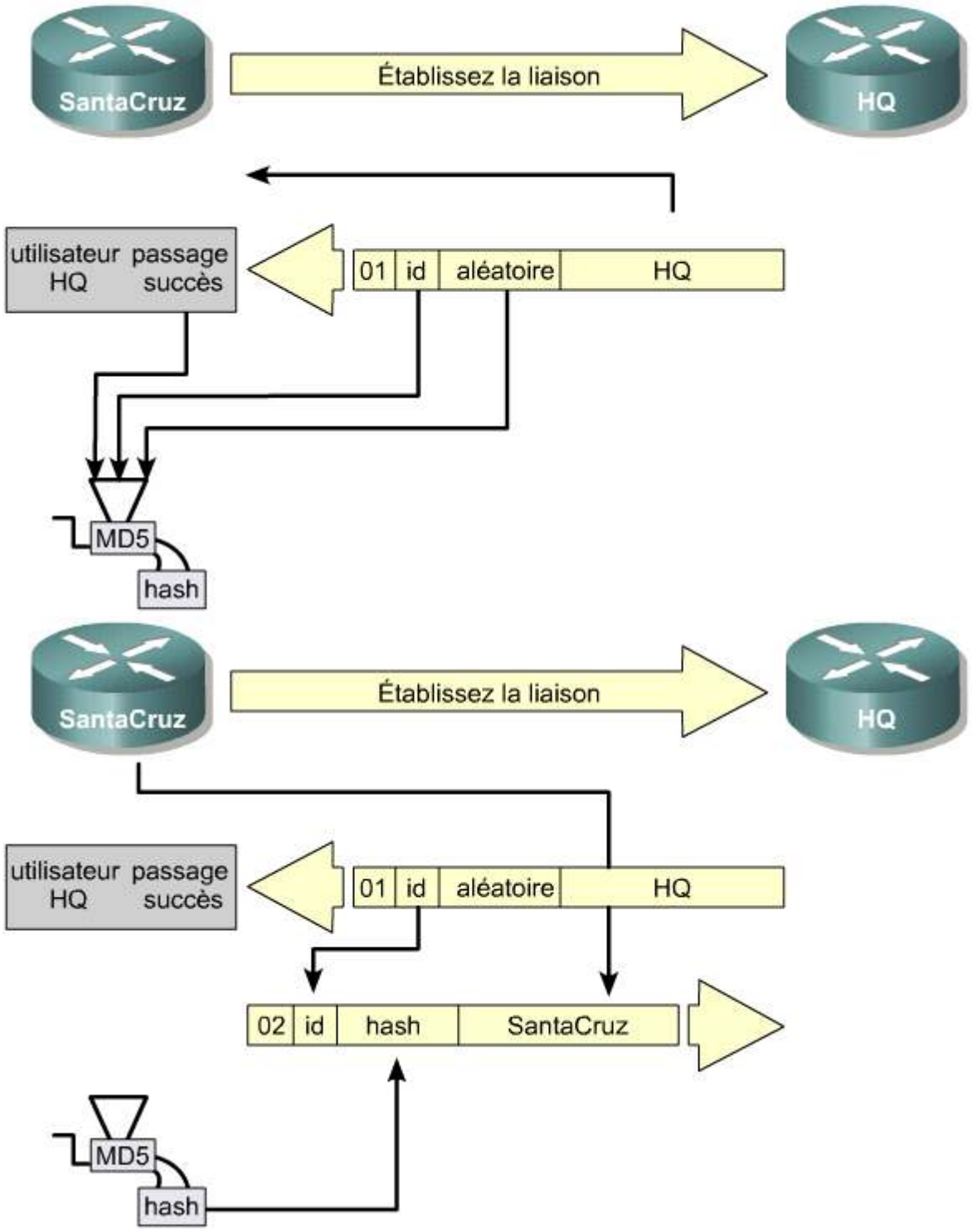


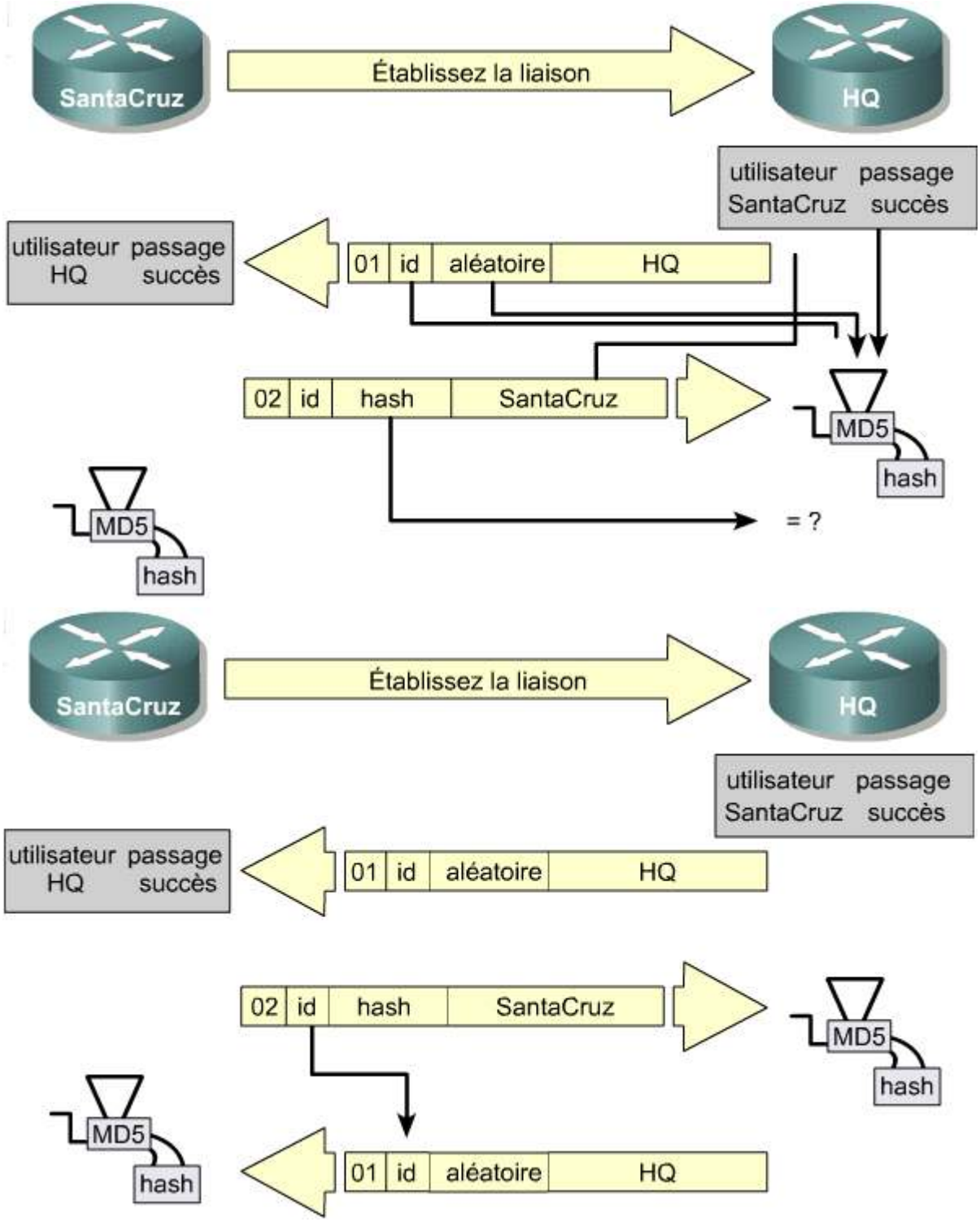
- La méthode d'authentification est déterminée.
- La base de données ou le serveur de sécurité local, qui contient une base de données de noms d'utilisateur et de mots de passe, est consulté pour déterminer si la paire nom d'utilisateur-mot de passe fournie concorde.
- Le processus vérifie la réponse d'authentification renvoyée par la base de données locale. En cas de réponse positive, la session PPP démarre. Si elle est négative, la session prend fin.

La figure 2 et la figure 3 correspondante détaillent le processus d'authentification CHAP.

Étape	Détail
A	Quand le routeur distant établit une liaison, les deux systèmes s'accordent pour utiliser l'authentification CHAP au cours de la négociation PPP LCP. Le routeur HQ interroge le routeur SantaCruz.
B	Le paquet d'interrogation est envoyé au routeur SantaCruz. Le nom du routeur HQ est utilisé pour authentifier le routeur HQ auprès du routeur SantaCruz.
C	Le nom de la source de l'interrogation, c'est-à-dire le routeur HQ, est utilisé pour rechercher le mot de passe dans la base de données locale. Le générateur de codes de hachage (MD5) produit une valeur à partir des informations reçues dans le paquet d'interrogation et du mot de passe associé au nom du routeur HQ. Cette valeur hachée est utilisée pour répondre à l'interrogation.
D	La valeur du paquet d'interrogation haché, le nom du routeur SantaCruz et l'ID de l'interrogation sont utilisés pour créer le paquet de réponse.
E	La source de l'interrogation introduit les mêmes valeurs d'interrogation que le routeur SantaCruz dans le générateur d'empreinte digitale. Ces valeurs d'interrogation incluent l'ID, le numéro aléatoire obtenu par l'interrogation d'origine et le mot de passe associé au nom SantaCruz. Par conséquent, les mots de passe des deux systèmes doivent être identiques. La source de l'interrogation compare son calcul à la valeur hachée reçue du routeur SantaCruz. Si les valeurs sont identiques, l'authentification réussit.
F	Si l'authentification échoue, un paquet d'échec CHAP est créé à partir des composants ci-dessous : · 04 = Type de message d'échec CHAP · id = copiée dans le paquet de réponse · " Échec de l'authentification " ou un message de texte similaire, censé être une explication lisible par l'utilisateur




SantaCruz
Établissez la liaison
HQ
utilisateur passage
HQ succès
01 id aléatoire HQ
MD5
hash
SantaCruz
Établissez la liaison
HQ
utilisateur passage
HQ succès
01 id aléatoire HQ
02 id hash SantaCruz
MD5
hash



Activité de média interactive

Glisser-Positionner: Processus d'authentification et d'encapsulation PPP

À la fin de cette activité, l'étudia connaîtra les étapes du processus d'authentification PPP.

3.3 Configuration de PPP

3.3.1 Présentation de la configuration de PPP

Les aspects configurables de PPP incluent les méthodes d'authentification, la compression, la détection d'erreurs et la prise en charge ou non de la multiliaison. La section ci-après décrit les différentes options de configuration de PPP.

Les routeurs Cisco qui utilisent l'encapsulation PPP peuvent inclure les options de configuration LCP décrites à la figure 1.

Options	Fonction	Protocole	Commande
Authentification	Les options d'authentification demandent que le côté appelant de la liaison entre des informations qui permettent d'assurer que l'émetteur dispose de l'autorisation de l'administrateur réseau pour effectuer l'appel. Les routeurs homologues échangent des messages d'authentification. PAP et CHAP constituent deux solutions alternatives.	PAP CHAP	`ppp authentication pap` `ppp authentication chap`
Compression	Les options de compression augmentent le débit effectif des connexions PPP en réduisant la quantité de données sur la trame qui doit traverser la liaison. Le protocole décompresse la trame à l'arrivée. Les deux protocoles de compression disponibles sur les routeurs Cisco sont Stacker et Predictor.	Stacker ou Predictor	`compress stac` `compress predictor`
Détection	Les mécanismes de détection d'erreur de PPP permettent à un processus d'identifier les conditions d'erreur. Les options Quality et Magic Number aident à assurer que la liaison de données reste fiable et sans boucle.	Quality Magic Number	`ppp quality <number 1-100>`
Multiliaison	Cisco IOS version 11.1 et ultérieures prennent en charge le protocole multiliaison. Cette fonction est parfois appelée PPP multiliaison. Cette autre possibilité fournit un équilibrage de la charge sur les interfaces routeur utilisées par PPP. Le protocole multiliaison effectue une fragmentation et un séquençage qui divisent la charge de PPP et envoie des fragments sur des circuits parallèles. Ce " faisceau " de canalisations PPP multiliaisons fonctionne comme une liaison logique unique, améliorant ainsi le débit et réduisant la latence entre les routeurs homologues.	MP	`ppp multilink`

3.3 Configuration de PPP

3.3.2 Configuration de PPP

L'exemple suivant permet l'encapsulation de PPP sur l'interface série 0/0:

```
Router#configure terminal
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
```

La compression logicielle point-à-point peut être configurée sur les interfaces série qui utilisent l'encapsulation PPP. La compression est effectuée de façon logicielle et peut avoir un effet considérable sur les performances du système. La compression n'est pas recommandée si le trafic est essentiellement constitué de fichiers compressés.

Pour configurer la compression sur PPP, entrez les commandes suivantes: 1

```
Router(config-if)#compress [predictor | stac]
```

Mot-clé	Description
Predictor	(Facultatif) Spécifie qu'un algorithme de compression Predictor va être utilisé.
Stac	(Facultatif) Spécifie qu'un algorithme de compression Stacker (LZS) va être utilisé.

```
Router(config-if)#ppp quality percentage
```

Mot-clé	Description
Percentage	Spécifie le seuil de qualité de la liaison. La plage varie de 1 à 100.

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#compress [predictor | stac]
```

Entrez les commandes suivantes pour surveiller les données reçues sur la liaison et éviter que la trame ne tourne en boucle:

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp quality percentage
```

Les commandes ci-dessous procèdent à un équilibrage de la charge sur plusieurs liaisons:

```
Router(config)#interface serial 0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp multilink
```

Activité de TP

Exercice: Configuration de l'encapsulation PPP

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs Washington et Dublin au moyen du protocole PPP.

Activité de TP

Activité en ligne: Configuration de l'encapsulation PPP

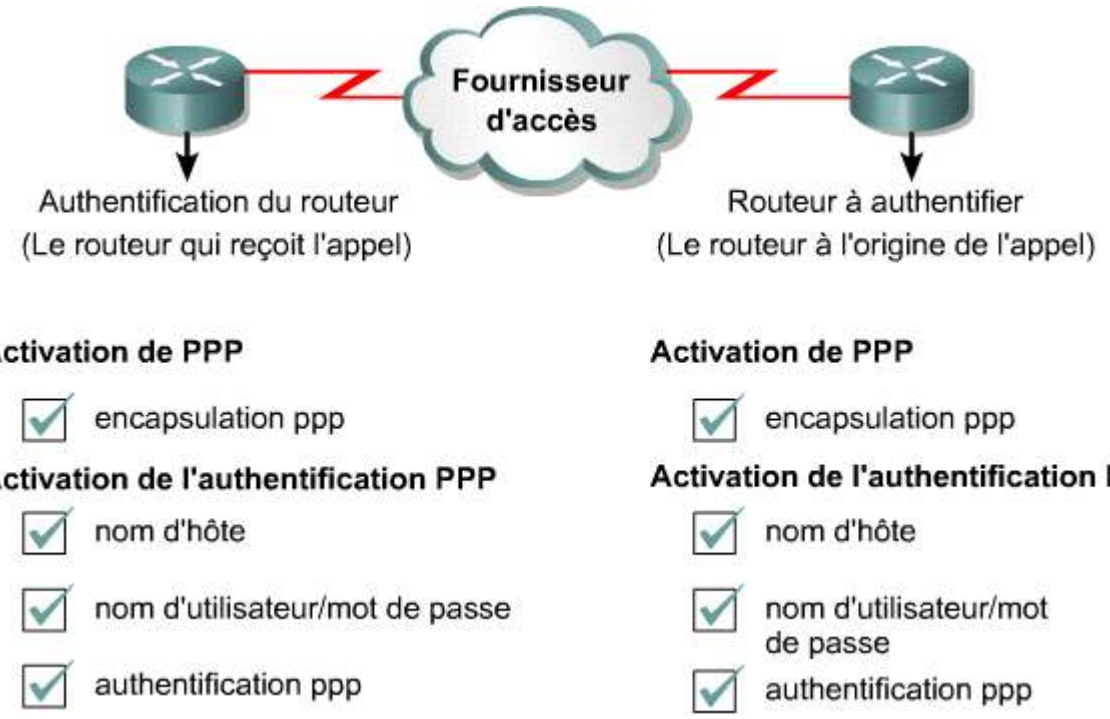
Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs Washington et Dublin au moyen du protocole PPP.

3.3 Configuration de PPP

3.3.3 Configuration de l'authentification PPP

La procédure présentée dans le tableau décrit la configuration de l'encapsulation PPP et des protocoles d'authentification PAP/CHAP. [1] [2]

Étape	Description
Étape 1	Définissez sur chaque routeur le nom d'utilisateur et le mot de passe prévu pour le routeur distant : `Router(config)#username name password secret` Description des arguments : • *name*-This is the host name of the remote router. Remarque : Les majuscules et les minuscules sont différenciées pour le nom d'hôte. • *secret*-Sur les routeurs Cisco, le mot de passe secret doit être identique sur les deux routeurs.
Étape 2	Passez en mode de configuration d'interface pour l'interface voulue.
Étape 3	Configurez l'interface pour l'encapsulation PPP : `Router(config-if)#encapsulation ppp`
Étape 4	Configurez l'authentification PPP : `Router(config-if)#ppp authentication {chap | chap pap | pap chap | pap}`
Étape 5	Si les protocoles CHAP et PAP sont activés, la première méthode indiquée est demandée pendant la phase de négociation de la liaison. Si l'homologue refuse la première méthode ou suggère la deuxième, cette dernière est essayée.
Étape 6	Dans Cisco IOS versions 11.1 ou ultérieures, PAP doit être activé sur l'interface, car il est désactivé par défaut. `Router(config-if)#ppp pap sent-username username password password`



Il est essentiel de procéder à une configuration correcte, car PAP et CHAP s'appuient sur ces paramètres pour leur authentification.

La figure 1 est un exemple de configuration de l'authentification PAP bidirectionnelle. Les deux routeurs authentifient et sont authentifiés, de telle sorte qu'un effet de miroir se produise sur les commandes d'authentification PAP. Le nom d'utilisateur et le mot de passe PAP que chaque routeur envoie doit correspondre à ceux spécifiés à l'aide de la commande **`username nom password mot de passe`** de l'autre routeur.

Le protocole PAP procure une méthode simple permettant à un nœud distant d'établir son identité à l'aide d'un échange en deux étapes. Ceci s'effectue uniquement à l'établissement initial de la liaison. Le nom d'hôte d'un routeur doit concorder avec le nom d'utilisateur que l'autre routeur a configuré. Les mots de passe doivent également correspondre. 3

```
hostname Left
username Right password
sameone
!
int serial 0/0
ip address 128.0.1.1
255.255.255.0
encapsulation ppp
ppp authentication PAP
ppp pap sent-username
Left
password sameone
```

```
hostname Right
username Left password
sameone
!
int serial 0/0
ip address 128.0.1.2
255.255.255.0
encapsulation ppp
ppp authentication PAP
ppp pap sent-username
Right
password sameone
```

Le protocole d'authentification à échanges confirmés (CHAP) permet de vérifier régulièrement l'identité du nœud distant à l'aide d'un échange en trois étapes. Le nom d'hôte d'un routeur doit concorder au nom d'utilisateur que l'autre routeur a configuré. Les

mots de passe doivent également correspondre. La vérification a lieu lors de l'établissement initial de la liaison et peut être répétée à tout moment une fois la liaison établie. 4

```
hostname Left
username Right password
sameone
!
int serial 0/0
ip address 128.0.1.1
255.255.255.0
encapsulation ppp
ppp authentication CHAP
```

```
hostname Right
username Left password
sameone
!
int serial 0/0
ip address 128.0.1.2
255.255.255.0
encapsulation ppp
ppp authentication CHAP
```

Activité de TP

Exercice: Configuration de l'authentification PPP

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs Madrid et Tokyo.

Activité de TP

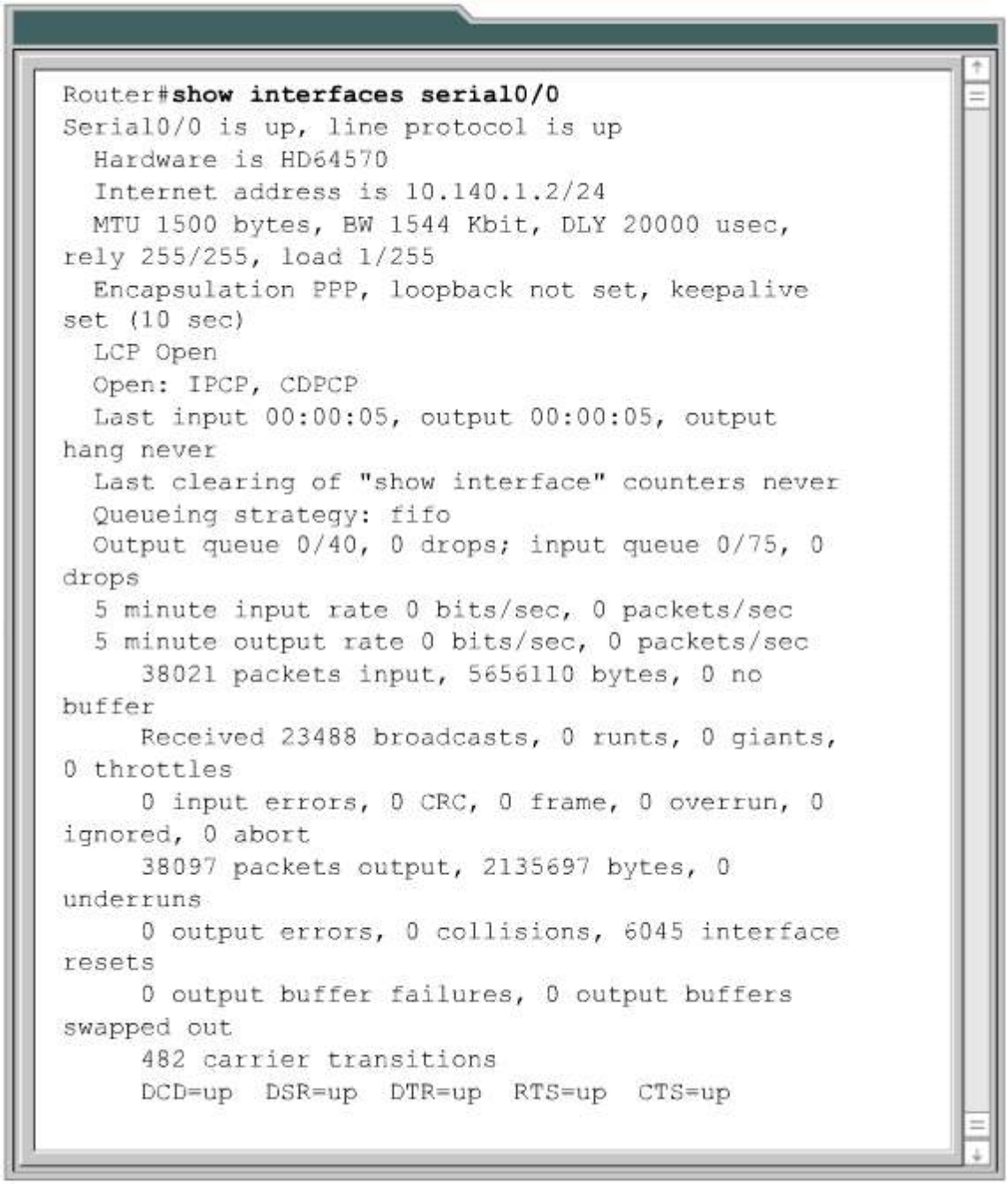
Activité en ligne: Configuration de l'authentification PPP

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs Madrid et Tokyo.

Activité de TP

Activité en ligne: username nom password mot de passe

Au cours de cette activité, l'étudiant va démontrer l'utilisation de la commande **`username nom password mot de passe`**.


Router#show interfaces serial0/0
Serial0/0 is up, line protocol is up
Hardware is HD64570
Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive
set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:05, output 00:00:05, output
hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0
drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
38021 packets input, 5656110 bytes, 0 no
buffer
Received 23488 broadcasts, 0 runts, 0 giants,
0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored, 0 abort
38097 packets output, 2135697 bytes, 0
underruns
0 output errors, 0 collisions, 6045 interface
resets
0 output buffer failures, 0 output buffers
swapped out
482 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

Utilisez la commande **show interfaces serial** pour vérifier la configuration de l'encapsulation HDLC ou PPP. Les résultats de la commande, à la figure 1, illustrent une configuration PPP. Quand le protocole HDLC (*high-level data link control*) est configuré, «Encapsulation HDLC» doit apparaître dans les résultats renvoyés par la commande **show interfaces serial**. Lorsque PPP est configuré, ses états LCP (Link Control Protocol) et NCP (Network Control Protocol) peuvent être vérifiés à l'aide de la commande **show interfaces serial**.

Commande	Description
encapsulation ppp	Active PPP sur une interface.
ppp authentication pap	Active l'authentification PAP sur une interface
ppp authentication chap	Active l'authentification CHAP sur une interface
username *username* **password** *password*	Établit un système d'authentification s'appuyant sur les
show interfaces	Affiche des statistiques sur toutes les interfaces configurées du routeur ou du serveur d'accès
debug ppp authentication	Débogue le processus d'authentification PAP ou CHAP
undebug all	Désactive tous les écrans de débogage

La figure 2 répertorie les commandes utilisées pour activer, configurer et vérifier PPP.

Activité de TP

Exercice: Vérification de la configuration de PPP

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs Brasilia et Warsaw au moyen du protocole PPP.

Activité de TP

Activité en ligne: Vérification du protocole PPP

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs Brasilia et Warsaw au moyen du protocole PPP.

3.3 Configuration de PPP

3.3.5 Dépannage de la configuration de l'encapsulation série

```
4d20h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
4d20h: Se0/0 PPP: Treating connection as a dedicated line
4d20h: Se0/0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0/0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0/0 CHAP: I CHALLENGE id 3 len 28 from "right"
4d20h: Se0/0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0/0 CHAP: I RESPONSE id 2 len 28 from "right"
4d20h: Se0/0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0/0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
```

La commande **debug ppp authentication** affiche la séquence d'échange d'authentification. La figure 1 illustre les résultats renvoyés par le routeur de gauche au cours de l'authentification CHAP avec le routeur de droite, quand **debug ppp**

authentication est activée. Lorsque l'authentification bidirectionnelle est configurée, chaque routeur authentifie l'autre. Des messages s'affichent pour le processus authentifiant et le processus authentifié. Utilisez la commande **debug ppp authentication** pour afficher la séquence d'échange au moment où elle se produit.

Affichage	Description
Se0/0 PPP : Phase is AUTHENTICATING, by both	Authentification bidirectionnelle
Se0/0 PPP : O AUTH-REQ id 4 len 18 from "left"	Requête d'identification sortante
Se0/0 PPP : O AUTH-REQ id 1 len 18 from "right"	Requête d'authentification entrante
Se0/0 PPP : Authenticating peer right	Authentification entrante
Se0/0 PPP : O AUTH-ACK id 1 len 5	Accusé de réception sortant
Se0/0 PPP : O AUTH-ACK id 4 len 5	Accusé de réception entrant

La figure 2 présente les résultats renvoyés par le routeur pour une authentification PAP bidirectionnelle.

La commande **debug ppp** sert à afficher des informations sur le fonctionnement de PPP. La forme **no** de cette commande désactive l'affichage du message de débogage. 3

Commande	Description
packet	S'utilise avec la commande **debug ppp** pour afficher les paquets PPP envoyés et reçus
negotiation	S'utilise avec la commande **debug ppp** pour afficher les paquets PPP transmis au démarrage de PPP, où les options PPP sont négociées
error	S'utilise avec la commande **debug ppp** pour afficher les erreurs de protocole et les statistiques d'erreur associées à la négociation et à l'utilisation de la connexion PPP
chap	S'utilise avec la commande **debug ppp** pour afficher les échanges de paquets CHAP (Challenge Authentication

```
Router#debug ppp {authentication | packet | negotiation | error | chap}
Router#no debug ppp {authentication | packet | negotiation | error | chap}
```

Activité de TP

Exercice: Dépannage de la configuration de PPP

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs London et Paris, ainsi que dépanner la connexion.

Activité de TP

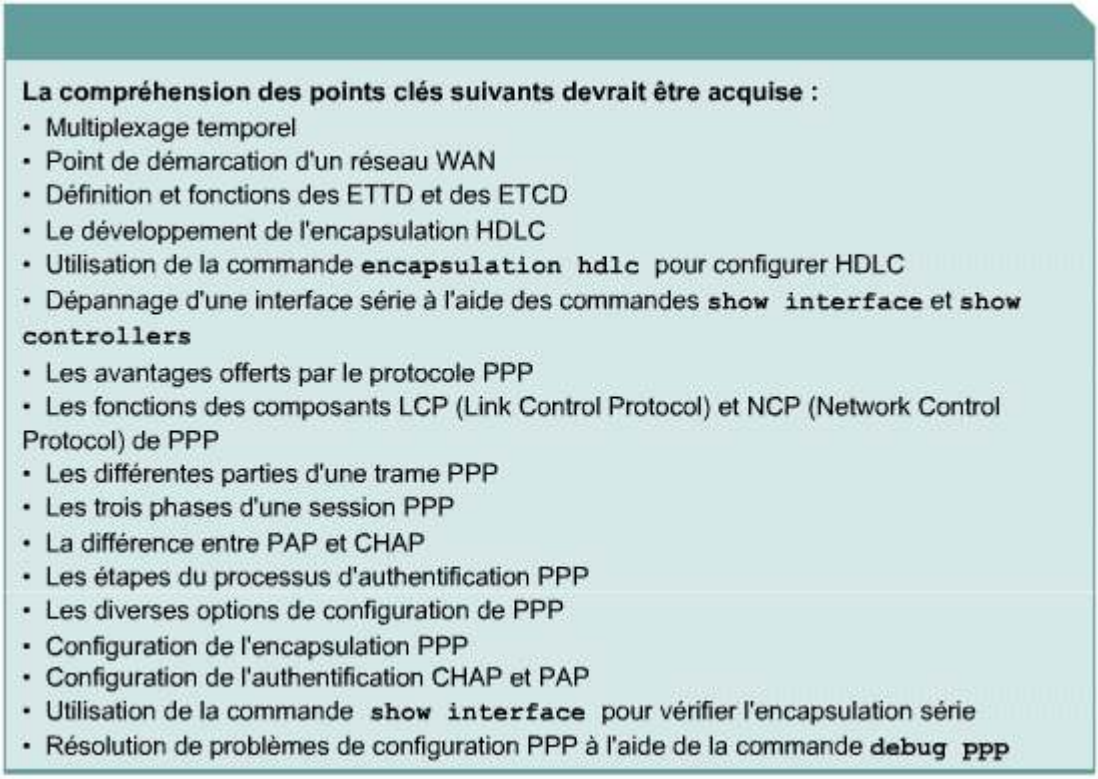
Activité en ligne: Dépannage d'une interface série

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs London et Paris, puis utiliser les commandes show pour résoudre les problèmes de connectivité.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Le multiplexage temporel
- Le point de démarcation d'un réseau WAN
- La définition et les fonctions des ETTD et des ETCD
- Le développement de l'encapsulation HDLC
- L'utilisation de la commande **`encapsulation hdlc`** pour configurer HDLC
- Le dépannage d'une interface série avec les commandes **`show interface`** et **`show controllers`**
- Les avantages offerts par le protocole PPP
- Les fonctions des composants LCP (*Link Control Protocol*) et NCP (Network Control Protocol) de PPP
- Les différentes parties d'une trame PPP
- Les trois phases d'une session PPP
- La différence entre PAP et CHAP
- Les étapes du processus d'authentification PPP
- Les diverses options de configuration de PPP
- La configuration de l'encapsulation PPP
- La configuration de l'authentification CHAP et PAP
- L'utilisation de la commande **`show interface`** pour vérifier l'encapsulation série
- La résolution de problèmes de configuration PPP à l'aide de la commande **`debug ppp`**


La compréhension des points clés suivants devrait être acquise :
• Multiplexage temporel
• Point de démarcation d'un réseau WAN
• Définition et fonctions des ETTD et des ETCD
• Le développement de l'encapsulation HDLC
• Utilisation de la commande encapsulation hdlc pour configurer HDLC
• Dépannage d'une interface série à l'aide des commandes show interface et show controllers
• Les avantages offerts par le protocole PPP
• Les fonctions des composants LCP (Link Control Protocol) et NCP (Network Control Protocol) de PPP
• Les différentes parties d'une trame PPP
• Les trois phases d'une session PPP
• La différence entre PAP et CHAP
• Les étapes du processus d'authentification PPP
• Les diverses options de configuration de PPP
• Configuration de l'encapsulation PPP
• Configuration de l'authentification CHAP et PAP
• Utilisation de la commande show interface pour vérifier l'encapsulation série
• Résolution de problèmes de configuration PPP à l'aide de la commande debug ppp

Vue d'ensemble

Le réseau RNIS (*Réseau numérique à intégration de services*) fournit une connectivité numérique de bout en bout et prend en charge une large gamme de services, notamment vocaux et de données.

Avec RNIS, plusieurs canaux numériques fonctionnent simultanément sur le câblage téléphonique ordinaire utilisé pour les lignes analogiques, mais le signal transmis est numérique, et non analogique. La latence est bien moins élevée sur une ligne RNIS qu'elle ne l'est sur une ligne analogique.

Le routage à établissement de connexion à la demande (DDR – *Dial-on-demand routing*) est une technique développée par Cisco pour constituer un réseau longue distance (WAN) sur les lignes téléphoniques existantes au lieu de lignes dédiées distinctes. Les réseaux téléphoniques publics commutés (RTPC) sont impliqués dans ce processus.

DDR s'utilise quand il n'est pas nécessaire de disposer d'une connexion constante et permet donc de réduire les coûts. DDR définit le processus d'un routeur qui se connecte via un réseau téléphonique quand il y a du trafic à envoyer, puis qui se déconnecte à la fin du transfert.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Définir les normes RNIS utilisées pour l'adressage, les concepts et la signalisation
- Décrire la manière dont RNIS utilise les couches physique et de liaison de données
- Énumérer les interfaces et les points de référence de RNIS
- Configurer l'interface RNIS du routeur
- Déterminer le trafic autorisé en configurant DDR
- Configurer des routes statiques pour DDR
- Choisir le type d'encapsulation approprié à DDR
- Être capable de déterminer et d'appliquer une liste d'accès agissant sur le trafic DDR
- Configurer des interfaces de numérotation

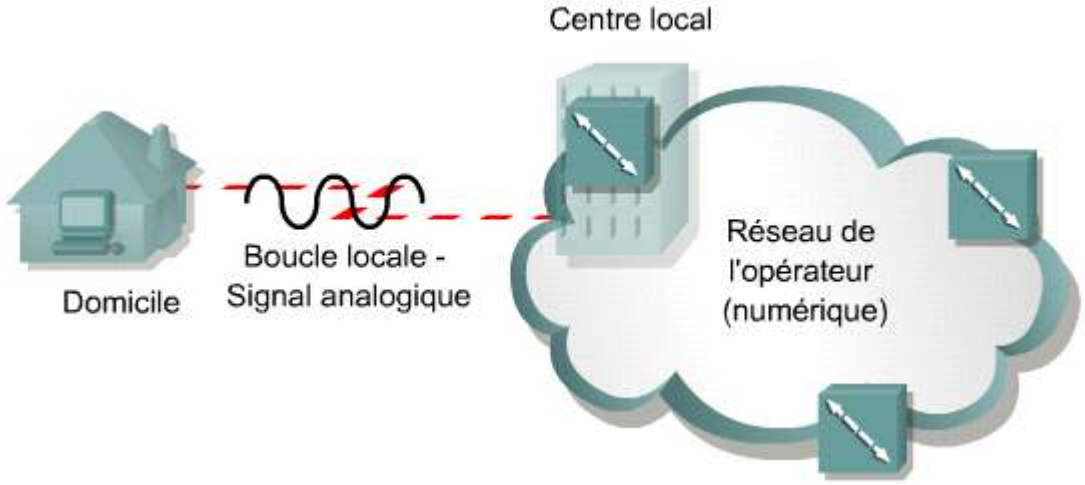
À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
4.1	Concepts RNIS
4.2	Configuration RNIS
4.3	Configuration DDR

4.1 Concepts RNIS

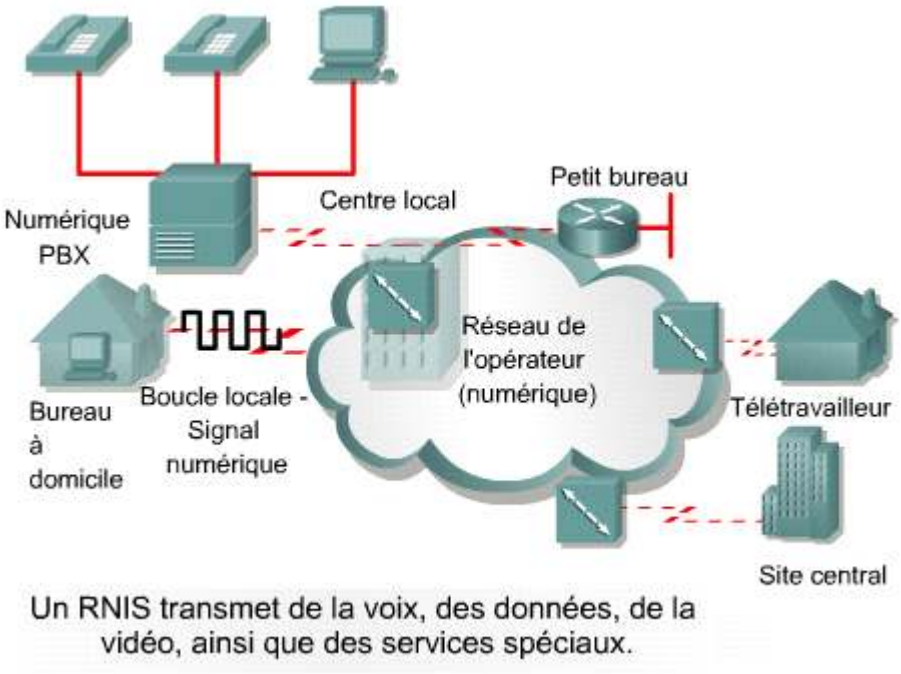
4.1.1 Présentation de RNIS

Plusieurs technologies WAN permettent d'accéder au réseau à partir de sites distants. RNIS est l'une d'entre elles. Cette technologie peut être utilisée pour résoudre les problèmes liés à une bande passante étroite, problèmes qui touchent les petits bureaux ou les utilisateurs faisant appel aux services téléphoniques commutés traditionnels.

Le RTPC traditionnel s'appuyait sur une connexion analogique entre les locaux du client et l'échange local, également appelée boucle locale. 1



Les circuits analogiques limitent la bande passante qui peut être obtenue sur la boucle locale. En effet, les restrictions des circuits ne permettent pas d'accepter les bandes passantes supérieures à environ 3000 Hz. La technologie RNIS permet d'utiliser des données numériques sur la boucle locale, et ainsi d'offrir de meilleurs débits aux utilisateurs distants. 2



Les opérateurs téléphoniques ont mis au point la technologie RNIS en vue de créer un réseau entièrement numérique. La technologie RNIS permet de transmettre des signaux numériques sur le câblage téléphonique existant. Ceci est seulement possible depuis que les commutateurs téléphoniques ont été mis à niveau pour prendre en charge les signaux numériques. La technologie RNIS s'utilise généralement pour le télétravail et pour connecter les petits bureaux distants au réseau local de l'entreprise.

Les opérateurs téléphoniques ont développé cette technologie en vue d'uniformiser les services proposés aux abonnés. Cela inclut l'interface UNI (*User-Network Interface*), mieux connue sous le nom de boucle locale. Les normes RNIS définissent le matériel et les méthodes d'établissement des appels assurant une connectivité numérique de bout en bout. Ces normes permettent d'obtenir une connectivité internationale en garantissant que les réseaux RNIS communiquent facilement entre eux. Dans un réseau RNIS, la numérisation s'opère sur le site de l'utilisateur et non au niveau de l'opérateur téléphonique.

La technologie RNIS permet de connecter des sites distants en numérique. Certains avantages du RNIS sont présentés ci-dessous: 3

Un RNIS est un ensemble de normes définissant un réseau numérique de bout en bout.

Avantages :
- Il transporte plusieurs types de trafic réseau (données, voix, vidéo).
- Il établit les communications plus rapidement qu'un service téléphonique de base.
- Le transfert des données est plus rapide qu'avec des modems.

- L'acheminement d'une grande diversité de signaux de trafic utilisateur, notamment données, voix et vidéo
- L'établissement des appels beaucoup plus rapide qu'avec une connexion modem
- Un meilleur taux de transfert que les modems grâce aux canaux B
- L'adaptation des canaux B aux liaisons PPP (*Point-to-Point Protocol*) négociées

Très souple, le service RNIS peut acheminer du trafic vocal, vidéo et de données. Il est possible d'utiliser plusieurs canaux pour acheminer différents types de trafics sur une seule connexion.

La technologie RNIS utilise la signalisation hors bande, le delta (canal D), pour l'établissement de l'appel et la signalisation. Pour un appel téléphonique normal, l'utilisateur compose le numéro un chiffre à la fois. Une fois que tous les numéros ont été reçus, l'appel peut être transmis à l'utilisateur distant. RNIS envoie les numéros au commutateur à la vitesse du canal D, ce qui accélère l'établissement de l'appel.

RNIS offre également une bande passante supérieure à une connexion commutée classique à 56 kbits/s. RNIS exploite des canaux Bearer, également appelés canaux B, comme des chemins de données entièrement dégagés. Chaque canal B offre un débit de 64 kbits/s. En utilisant plusieurs canaux B, la technologie RNIS offre aux utilisateurs une bande passante plus large sur les WAN que certaines lignes louées. Une connexion RNIS avec deux canaux B fournit une bande passante utilisable totale de 128 kbits/s.

Chaque canal B peut établir une connexion série distincte vers n'importe quel autre site du réseau RNIS. Comme le protocole PPP fonctionne à la fois sur des liaisons synchrones et asynchrones, les lignes RNIS peuvent être utilisées conjointement à l'encapsulation PPP.

4.1 Concepts RNIS
4.1.2 Normes et méthodes d'accès

L'établissement des premières normes RNIS date de la fin des années 1960. Une série complète de recommandations relatives aux réseaux RNIS a été publiée en 1984. L'Union internationale des télécommunications – Secteur de la normalisation des télécommunications (UIT-T), anciennement Comité consultatif international télégraphique et téléphonique (CCITT), en assure la mise à jour constante. Les normes RNIS sont un ensemble de protocoles relatifs à la téléphonie numérique et à la communication de données. L'ITU-T regroupe et organise les protocoles RNIS dans les catégories générales ci-dessous: 1

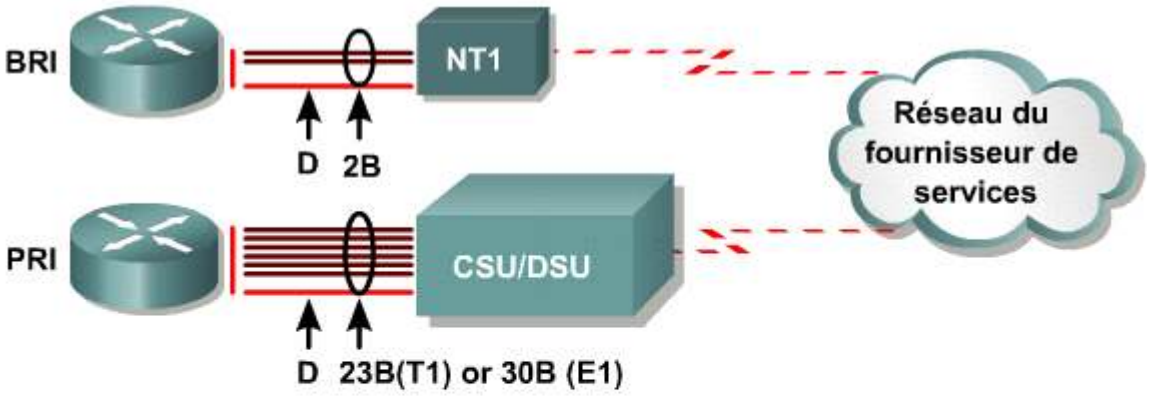
Objet	Protocole	Exemples clés
Réseau téléphonique et RNIS	Série E	E.164 – Plan de numérotation téléphonique international
Concepts, aspects et interfaces RNIS	Série I	I.100 Série - Concepts, Structures, Terminologie I.400 – Interfaces utilisateur-réseau
Commutation et signalisation	Série Q	Q.921 – Protocole de liaison LAPD Q.931 – Couche réseau RNIS entre le terminal et le commutateur

Normes ITU-T (ex CCITT)

- **Protocoles E** – Recommandent des normes sur le réseau téléphonique pour RNIS. Par exemple, le protocole E.164 décrit l'adressage international pour RNIS.

- **Protocoles I** – Traitent des concepts, de la terminologie et des méthodes générales. La série I.100 contient les concepts RNIS généraux, ainsi que la structure d'autres recommandations de la série I. I.200 traite des aspects services de RNIS. I.300 décrit les aspects réseau. I.400 explique comment est fournie l'interface UNI.
- **Protocoles Q** – Spécifient la manière dont la commutation et la signalisation doivent fonctionner. Dans le présent contexte, le terme signalisation désigne le processus d'établissement d'un appel RNIS.

Les normes RNIS définissent deux principaux types de canaux, chacun présentant une vitesse de transmission différente. Le canal Bearer, ou canal B, est défini comme un chemin numérique entièrement dégagé de 64 Kbits/s. On dit qu'il est entièrement dégagé car il peut servir à transmettre n'importe quel type de données numériques en mode full-duplex. Par exemple, un appel téléphonique vocal numérisé peut être transmis sur un seul canal B. Le deuxième type de canal est appelé le canal delta, ou canal D. Il peut y avoir 16 kbits/s pour l'accès de base BRI (*Basic Rate Interface*) ou 64 kbits/s pour l'accès primaire PRI (*Primary Rate Interface*). Le canal D sert à acheminer des informations de contrôle pour le canal B.



Canal	Capacité	Utilisé principalement pour
B	64 kbps	Les données à commutation de circuits (HDLC, PPP)
D	16/64 kbps	Les informations de signalisation (LAPD)

Lors de la mise en place d'une connexion TCP, un échange d'informations, appelé établissement de la connexion, s'effectue. Ces informations sont échangées sur le chemin par lequel les données vont ensuite être transmises. Les informations de contrôle et les données partagent toutes deux le même chemin. C'est ce que l'on appelle la signalisation in band. La technologie RNIS, elle, fait appel à un canal séparé pour les informations de contrôle, le canal D. C'est ce que l'on appelle la signalisation hors bande.

La norme RNIS spécifie deux méthodes d'accès standard, à savoir BRI et PRI. Une seule interface BRI ou PRI fournit un regroupement multiplexé de canaux B et D.

BRI utilise deux canaux B à 64 kbits/s, plus un canal D à 16 kbits/s. BRI fonctionne avec de nombreux routeurs Cisco. Comme ce mode utilise deux canaux B et un canal D, le BRI est parfois appelé 2B+D.

Les canaux B peuvent s'utiliser pour transmettre des voix numérisées. Dans ce cas, des méthodes spécialisées sont utilisées pour le codage de la voix. Par ailleurs, les canaux B peuvent être utilisés pour un acheminement de données à vitesse relativement élevée. Dans ce mode, les informations sont acheminées sous un format de trame, au moyen des protocoles de couche 2 HDLC (*high-level data link control*) ou PPP. Le protocole PPP est beaucoup plus robuste que la procédure HDLC dans la mesure où il fournit un mécanisme d'authentification et de négociation de la compatibilité des liens et de la configuration de protocoles.

On considère que la connexion RNIS est à commutation de circuits. C'est le canal B qui constitue l'unité élémentaire de commutation de circuits.

Le canal D achemine les messages de signalisation, tels que l'établissement et la fermeture de l'appel, pour contrôler les communications sur les canaux B. Le trafic sur le canal D utilise le protocole LAPD (*Link Access Procedure on the D Channel*). LAPD est un protocole de couche de liaison de données fondé sur HDLC.

En Amérique du Nord et au Japon, PRI offre vingt-trois canaux B à 64 kbits/s et un canal D à 64 kbits/s. Un accès PRI fournit donc le même service qu'une connexion T1 ou DS1. En Europe et dans la plus grande partie du reste du monde, le mode PRI

offre 30 canaux B et un canal D afin de fournir le même niveau de service qu'un circuit E1. PRI utilise une unité DSU/CSU (*Data Service Unit*/*Channel Service Unit*) pour les connexions T1/E1.

4.1 Concepts RNIS

4.1.3 Modèle en 3 couches et protocoles de la technologie RNIS

La technologie RNIS utilise un ensemble de normes de l'UIT-T portant sur la couche physique, la couche de liaison de données et la couche réseau du modèle de référence OSI. 1

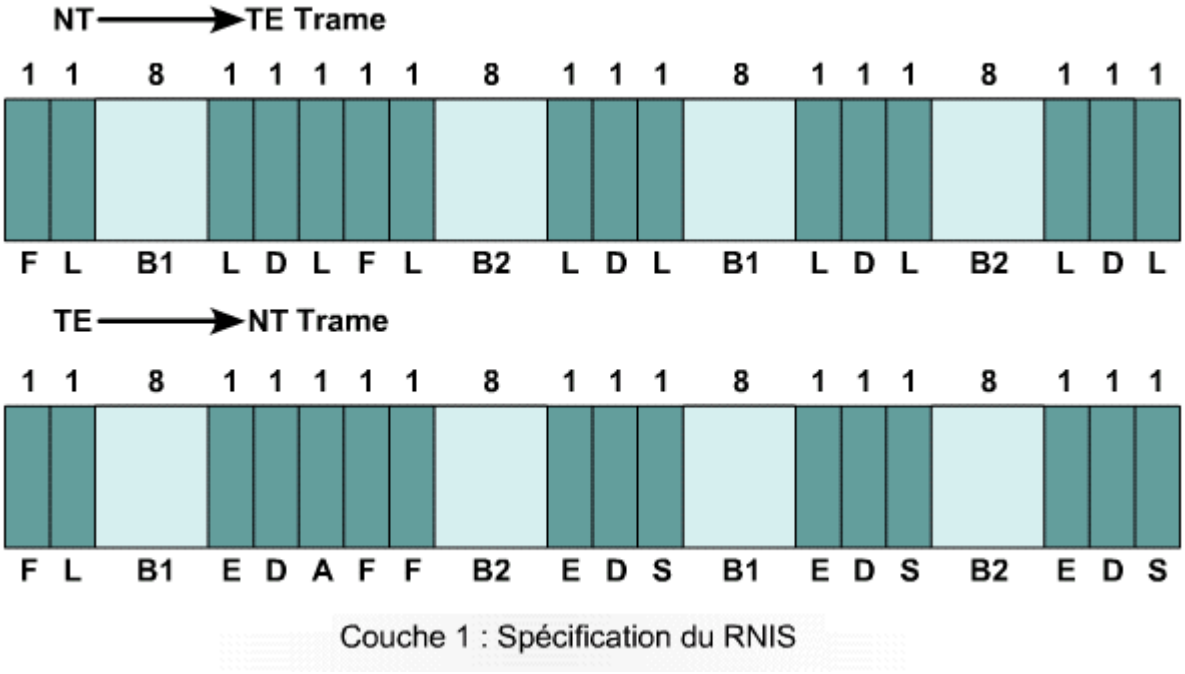
Couche OS	Canal D	Canal B
3	Q.931 – ISDN Couche réseau entre le terminal et le commutateur	IP
2	Q.921 – LAPD (Protocole de liaison LAPD)	PPP HDLC
1	I.430/I.431 - Interface de couche physique RNIS : = I.430 pour l'interface de base = I.431 pour l'interface primaire	

Un RNIS est défini au niveau des couches 1, 2 et 3 du modèle OSI.

- Les spécifications RNIS de la couche physique BRI et PRI sont définies respectivement dans les normes ITU-T I.430 et I.431.
- La spécification RNIS relative à la liaison de données est fondée sur le protocole LAPD et est formellement spécifiée dans les normes ci-dessous:
  - ITU-T Q.920
  - ITU-T Q.921
  - ITU-T Q.922
  - ITU-T Q.923
- La couche réseau RNIS est définie dans les normes ITU-T Q.930, également appelée I.450, et ITU-T Q.931, également appelée I.451. Ces normes définissent les connexions d'utilisateur à utilisateur, à commutation de circuits et à commutation de paquets.

Le service BRI est fourni sur une boucle locale de cuivre servant traditionnellement au service téléphonique analogique. Même s'il n'existe qu'un seul chemin physique pour un service BRI, il offre trois chemins d'informations distincts, 2B+D. Les informations de ces trois canaux sont multiplexées en un seul chemin physique.

Le format de trame de la couche RNIS physique, dite couche 1, diffère selon que la trame est entrante ou sortante. S'il s'agit d'une trame sortante, elle est envoyée du terminal au réseau. Les trames sortantes utilisent le format de trame TE. Si la trame est entrante, elle est envoyée du réseau au terminal. Les trames entrantes utilisent le format de trame NT. 2


NT TE Trame
1 1 8 1 1 1 1 1 8 1 1 1 8 1 1 1 8 1 1 1
F L B1 L D L F L B2 L D L B1 L D L B2 L D L
TE NT Trame
1 1 8 1 1 1 1 1 8 1 1 1 8 1 1 1 8 1 1 1
F L B1 E D A F F B2 E D S B1 E D S B2 E D S

Couche 1 : Spécification du RNIS

Chaque trame contient deux sous-trames, chacune contenant les éléments suivants:

- 8 bits du canal B1
- 8 bits du canal B2
- 2 bits du canal D
- 6 bits de surcharge

Les trames RNIS BRI contiennent donc 48 bits. Quatre mille de ces trames sont transmises chaque seconde. Chaque canal B, B1 et B2 offre une capacité de 8 * 4000 * 2 = 64 kbits/s. Le canal D a une capacité de 2 * 4000 * 2 = 16 kbits/s. Ceci représente 144 Kbits/s (B2+B1+D) pour un débit binaire total de l'interface physique RNIS BRI de 192 Kbits/s. Le reste du débit est constitué des bits de surcharge requis pour la transmission: 6 * 4000 * 2 = 48 kbits/s.

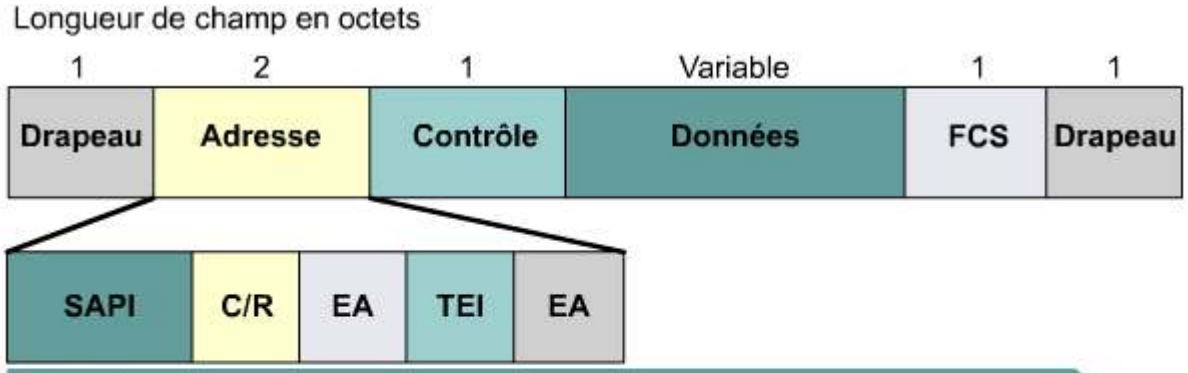
Les bits de surcharge d'une sous-trame RNIS sont utilisés de la façon suivante:

- **Bit de verrouillage de trame** – Synchronisation
- **Bit d'équilibrage de charge** – Ajustement de la valeur moyenne de bit
- **Écho des bits de canal D précédents** – Résolution des conflits pouvant survenir lorsque plusieurs terminaux sur un bus passif rivalisent pour un canal
- **Bit d'activation** – Activation des équipements
- **Bit de réserve** – Non affecté

Notez que le débit physique en bits de l'interface BRI est de 48*4000 = 192 kbits/s. Le débit effectif est de 144 kbits/s = 64 kbits/s + 64 kbits/s + 16 kbits/s (2B+D).

Le protocole LAPD constitue la couche 2 du canal de signalisation RNIS. Le protocole LAPD est semblable à HDLC. L'utilisation du protocole de liaison LAPD sur le canal D assure une circulation et une réception adéquates des flux d'information de contrôle et de signalisation.

Les champs d'indicateur et de contrôle du protocole LAPD sont identiques à ceux de HDLC. 3



Légende	
SAPI	Bits d'identification du point d'accès au service (6 bits)
C/R	Bit de commande/réponse
E/A	Bits d'adressage étendu
TEI	Identificateur de point d'extrémité

Couche 2 : Spécification du RNIS

Le champ d'adresse LAPD a une longueur de 2 octets. Le premier octet du champ d'adresse correspond à l'identificateur du point d'accès au service (*service access point identifier - SAPI*), qui indique le portail où les services LAPD sont fournis à la couche 3. Le bit de commande et de réponse (*command/response bit – C/R*) indique si la trame contient une commande ou une réponse. Le deuxième octet contient l'identificateur de point d'extrémité TEI (*Terminal Endpoint Identifier*). Les terminaux présents dans le local du client nécessitent tous un identificateur unique. Le TEI peut être attribué de façon statique à l'installation, ou de façon dynamique par le commutateur au démarrage de l'équipement. Si le TEI est assigné statiquement à l'installation, il est représenté par un nombre de 0 à 63. Les TEI assignés de façon dynamique varient de 64 à 126. Un TEI de 127, ou ne contenant que des 1, indique une diffusion broadcast.

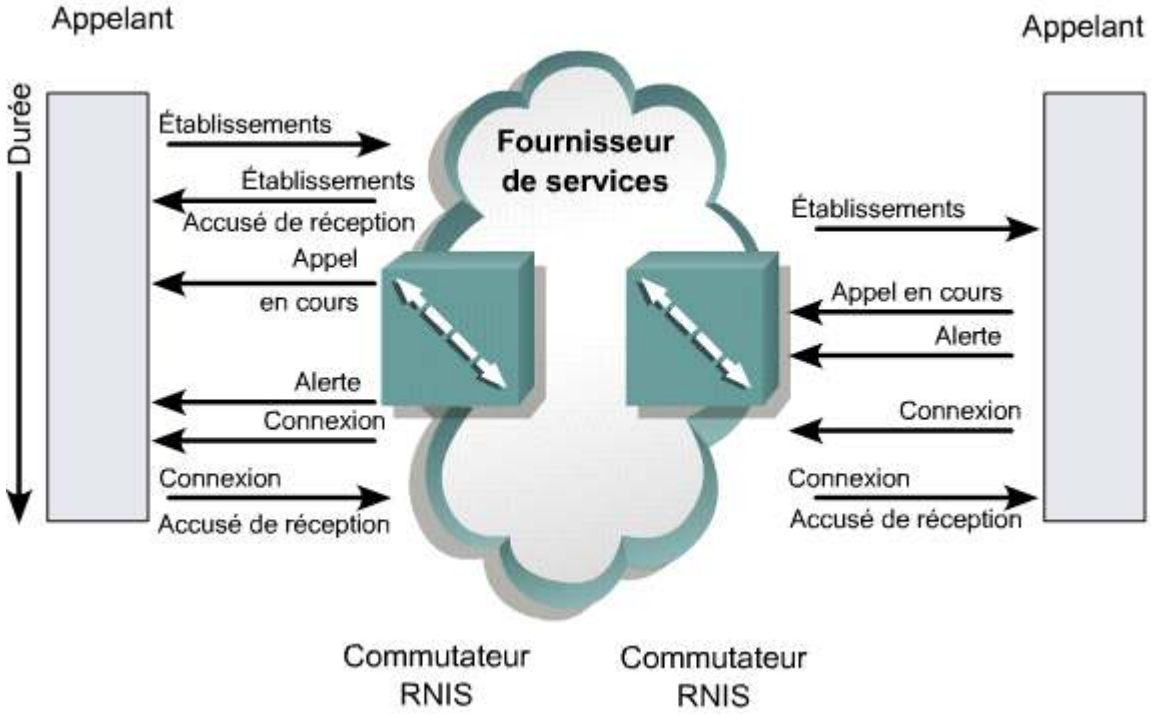
4.1 Concepts RNIS

4.1.4 Fonctions RNIS

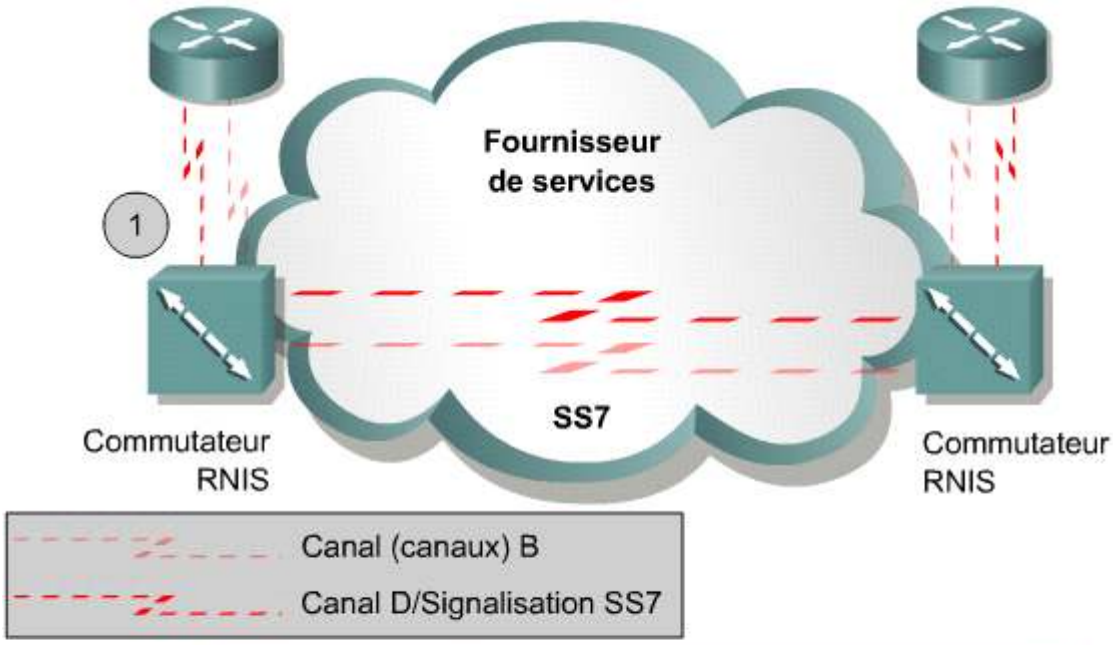
Plusieurs échanges doivent s'effectuer pour qu'un routeur se connecte à un autre par RNIS. Pour établir une connexion RNIS, c'est le canal D qui est utilisé entre le routeur et le commutateur RNIS. La signalisation SS7 (*Signal System 7*) est utilisée entre les commutateurs du réseau du fournisseur d'accès.

Le canal D entre le routeur et le commutateur RNIS est toujours en activité. La norme Q.921 décrit les processus de liaison de données RNIS du protocole LAPD, qui fonctionnent comme les processus de couche 2 du modèle de référence OSI. Le canal D s'utilise pour les fonctions de contrôle de communication, telles que l'établissement de l'appel, la signalisation et la fin de l'appel. Ces fonctions sont mises en œuvre dans le protocole Q.931. Q.931 spécifie les fonctions de la couche 3 du modèle de référence OSI. La norme Q.931 recommande une connexion de couche réseau entre l'extrémité terminale et le commutateur RNIS local, mais n'impose aucune recommandation de bout en bout. Comme certains commutateurs RNIS ont été développés avant que Q.931 ne soit normalisée, les différents fournisseurs RNIS et types de commutateurs utilisent diverses mises en œuvre de Q.931. Comme les types de commutateurs ne sont pas standard, la configuration des routeurs doit comporter des commandes spécifiant le commutateur RNIS sur lequel la connexion s'effectue.

La séquence d'événements ci-dessous s'effectue lors de l'établissement d'une communication BRI ou PRI: 1



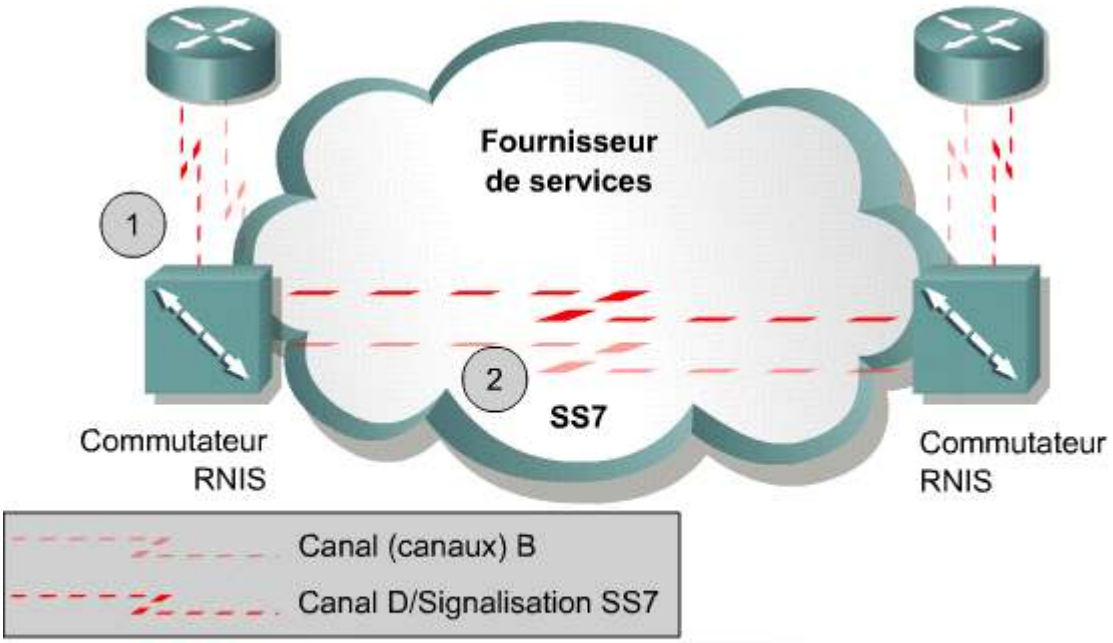
1. Le canal D est utilisé pour envoyer le numéro appelé au commutateur RNIS local. 2



Fenêtre contextuelle

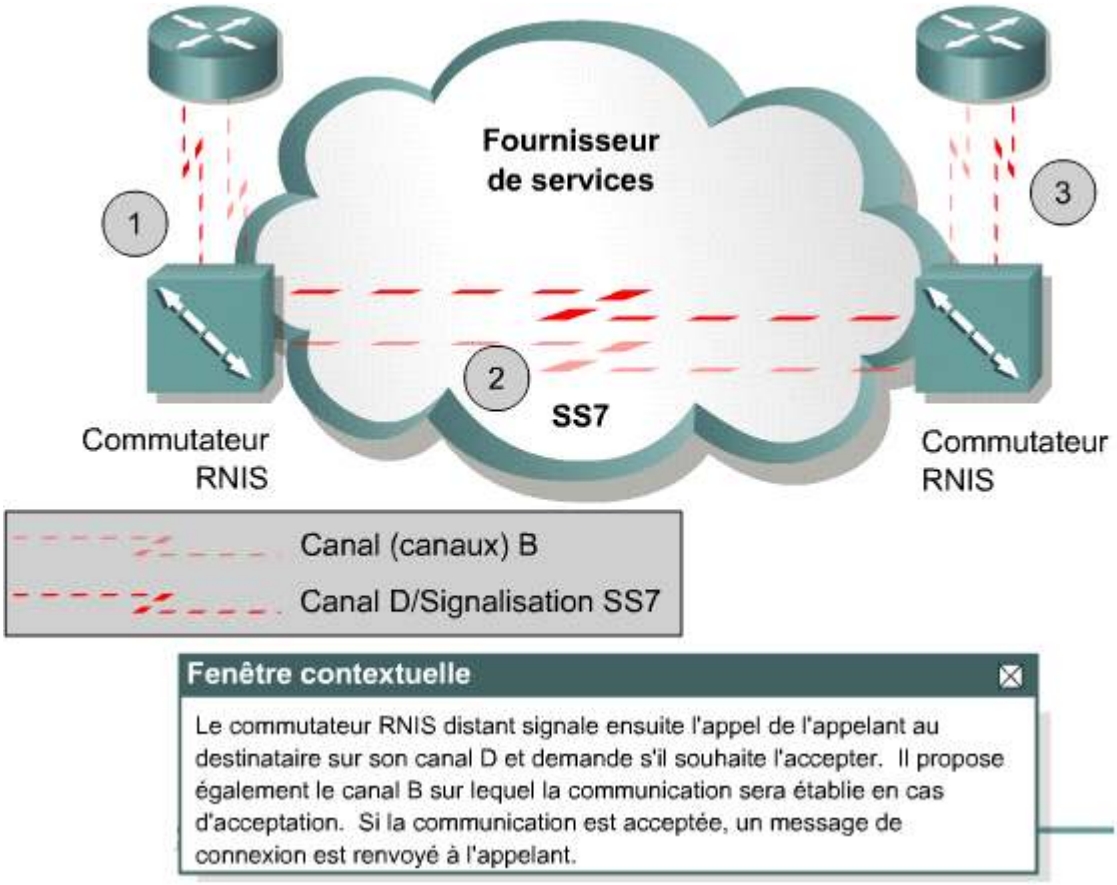
L'appelant initie un appel en envoyant un message d'établissement de communication au commutateur local. Ce message contient le numéro de l'équipement terminal (TE) RNIS avec lequel le routeur tente d'établir une communication. Ce message de contrôle est envoyé sur le canal D toujours actif.

2. Le commutateur local utilise le protocole de signalisation SS7 pour définir un chemin et transmettre le numéro appelé au commutateur RNIS distant. 3

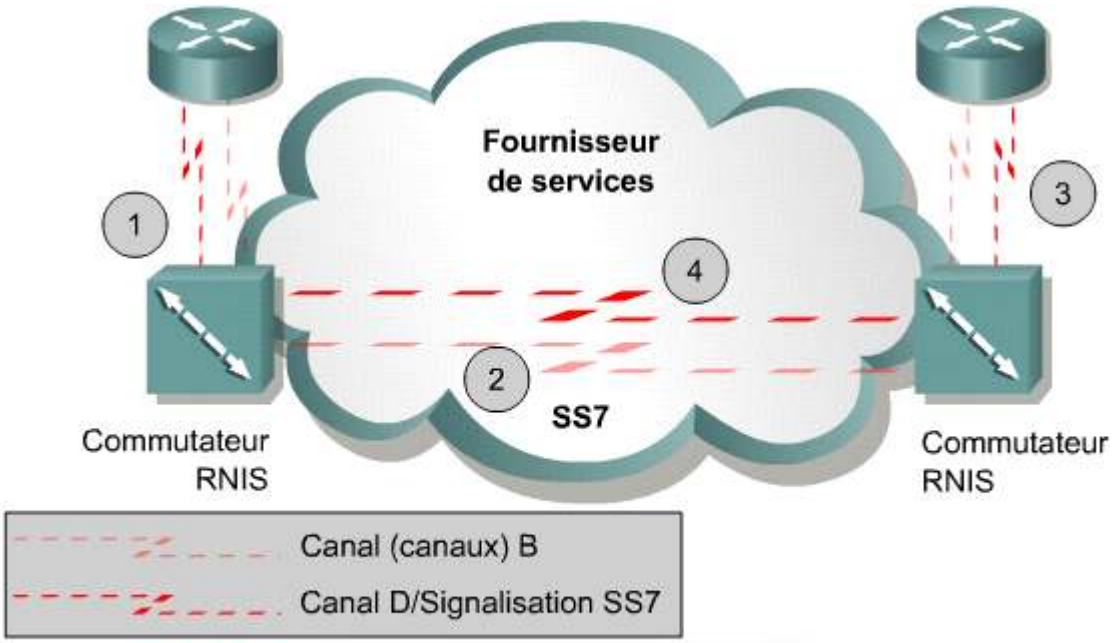


Sur le réseau de l'opérateur, un protocole distinct, SS7, est utilisé pour déterminer, à travers le nuage, un chemin vers le commutateur local pour le destinataire.

3. Le commutateur RNIS distant signale l'appel à la destination sur le canal D. 4

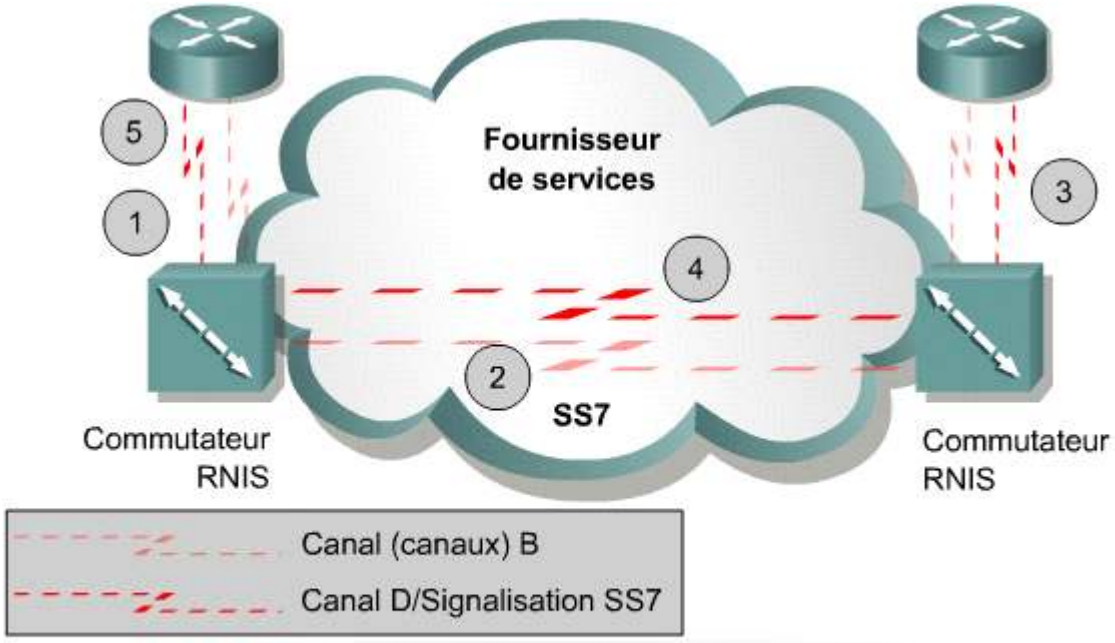

Fournisseur
de services
1
2
3
SS7
Commutateur
RNIS
Commutateur
RNIS
Canal (canaux) B
Canal D/Signalisation SS7
Fenêtre contextuelle
Le commutateur RNIS distant signale ensuite l'appel de l'appelant au destinataire sur son canal D et demande s'il souhaite l'accepter. Il propose également le canal B sur lequel la communication sera établie en cas d'acceptation. Si la communication est acceptée, un message de connexion est renvoyé à l'appelant.

4. L'équipement RNIS NT-1 de destination envoie un message de connexion d'appel au commutateur RNIS distant.
5. Le commutateur RNIS distant utilise SS7 pour envoyer un message de connexion d'appel au commutateur local. 5



SS7 retransmet le message de connexion d'appel au commutateur RNIS de l'appelant.

6. Le commutateur RNIS local connecte un canal B de bout en bout et laisse le deuxième canal B disponible pour une nouvelle conversation ou un transfert de données. Les deux canaux B peuvent être utilisés simultanément.



Le commutateur local indique à l'appelant que la communication a été établie. À ce stade, le commutateur indique à l'appelant que la communication a été établie sur le canal B1 ou B2.

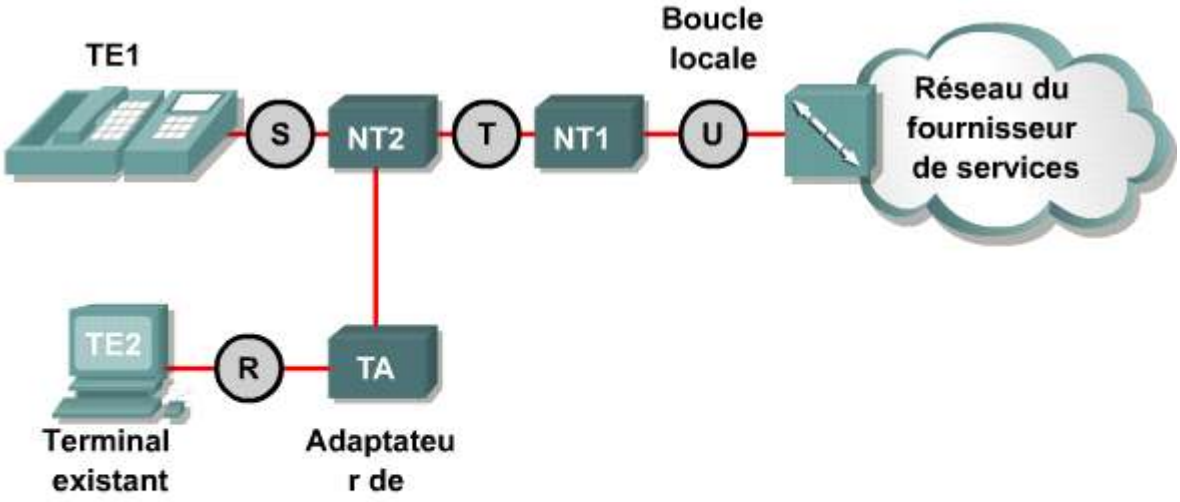
Activité de média interactive

Glisser-Positionner: Fonctions RNIS

À la fin de cette activité, l'étudiant sera en mesure d'identifier correctement le cycle d'établissement d'une communication RNIS.

4.1.5 Points de référence RNIS

Les normes RNIS définissent des groupes fonctionnels comme équipements ou matériel permettant à l'utilisateur d'accéder aux services de l'accès de base (BRI) ou de l'accès primaire (PRI). Les constructeurs peuvent créer des équipements prenant en charge une ou plusieurs fonctions. Les spécifications RNIS définissent quatre points de référence qui connectent un équipement RNIS à un autre. 1

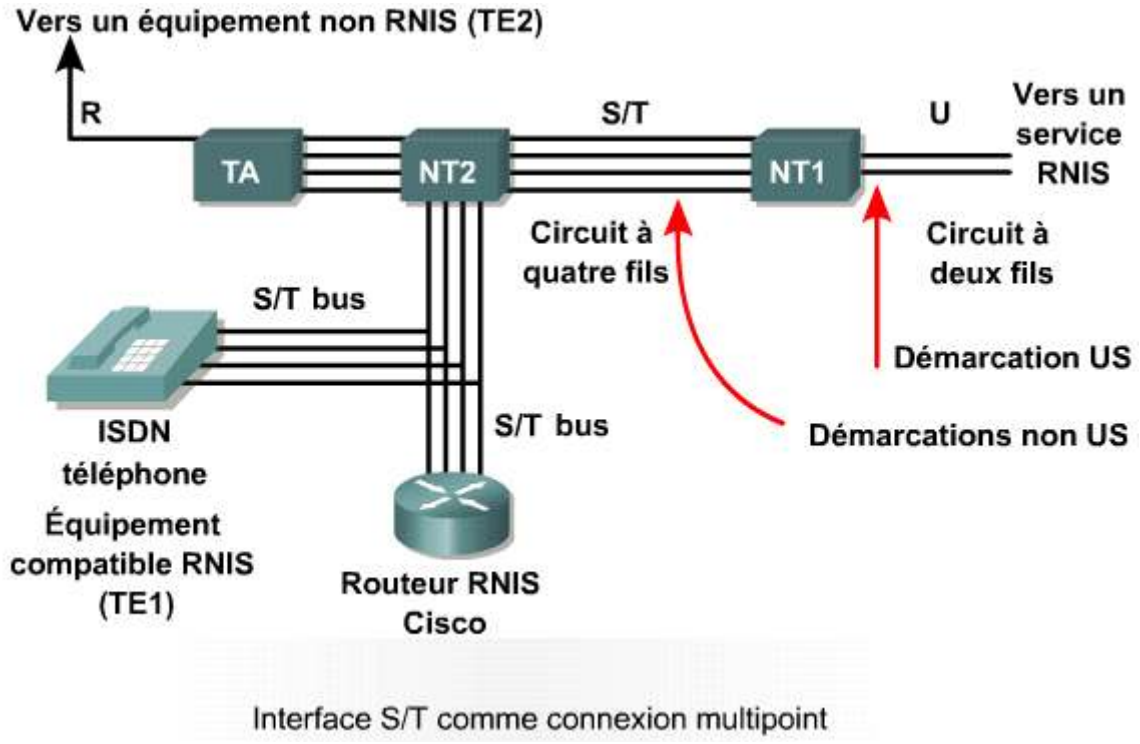


- Les groupes fonctionnels sont des équipements ou des composants matériels
- Les points de référence sont des démarcations ou des interfaces

Chaque unité d'un réseau RNIS effectue une tâche spécifique pour faciliter la connectivité de bout en bout. 2

Équipen	Type d'équipement	Fonction de l'équipeme
TE1	Équipement terminal 1	Désigne un équipement pourvu d'une interface RNIS native, tel qu'un routeur RNIS ou un téléphone RNIS.
TE2	Équipement terminal 2	Désigne un équipement non RNIS, tel qu'une station de travail ou un routeur, nécessitant un adaptateur de terminal pour se connecter à un fournisseur d'accès RNIS.
TA	Adaptateur de terminal	Convertit les signaux EIA/TIA-232, V.35 et autres en signaux BRI.
NT2	Terminaison de réseau 2	Point où s'opèrent le regroupement et la commutation de toutes les lignes RNIS d'un site client à l'aide d'une unité de commutation de l'abonné.
NT1	Terminaison de réseau 1	Contrôle les terminaisons électrique et physique du RNIS chez le client. Convertit les signaux BRI à quatre fils en signaux à deux fils utilisés par la ligne numérique RNIS.

Pour connecter des équipements exécutant des fonctions spécifiques, il est nécessaire de bien définir l'interface entre les deux équipements. On appelle ces interfaces des points de référence. 3



Interface S/T comme connexion multipoint

Les points de référence ci-dessous agissent sur le côté client de la connexion RNIS:

- **R** – Désigne la connexion entre un équipement terminal de type 2 non compatible RNIS (TE2) et un adaptateur de terminal (TA), par exemple une interface série RS-232.
- **S** – Désigne les points qui se connectent dans l'équipement de commutation du client aux terminaisons de réseau de type 2 (NT2) et permettent les appels entre les divers types d'équipements placés chez le client.
- **T** – Électriquement identique à l'interface S; désigne la connexion sortante entre la NT2 et le réseau RNIS ou la terminaison de réseau de type 1 (NT1).
- **U** – Désigne les connexions entre l'unité de terminaison de réseau de type 1 (NT1) et le réseau RNIS appartenant à la compagnie de téléphone.

Comme les références S et T sont similaires, certaines interfaces sont désignées par le sigle S/T. Bien qu'elles exécutent des fonctions différentes, le port est identique au niveau électrique et peut être utilisé pour n'importe laquelle de ces fonctions.

Activité de média interactive

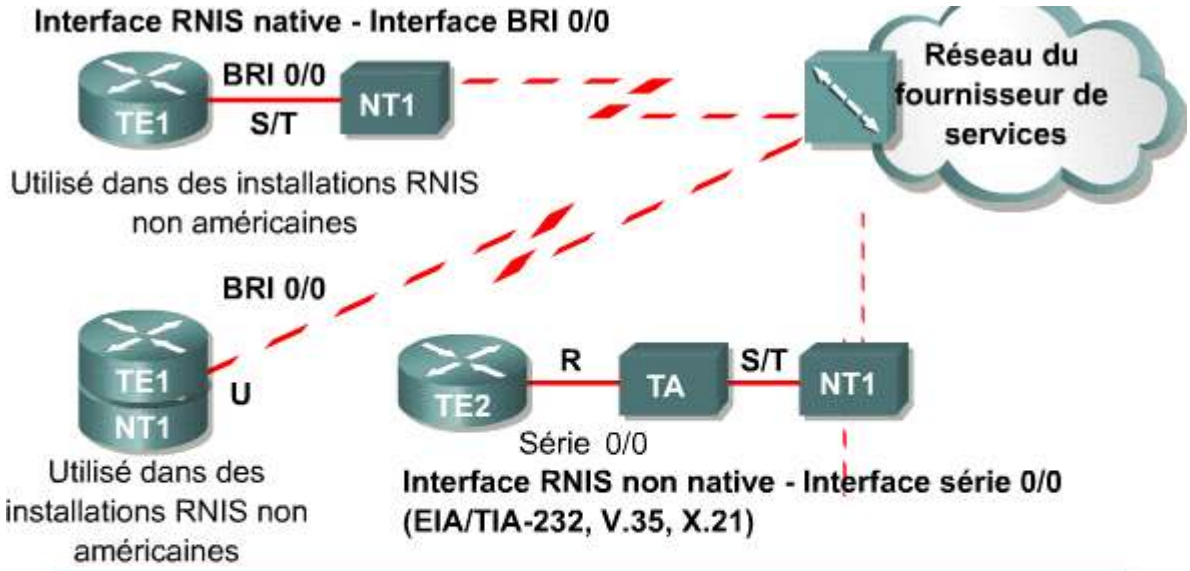
Glisser-Positionner: Points de référence RNIS

À la fin de cette activité, l'étudiant sera en mesure d'identifier correctement les points de référence RNIS.

4.1 Concepts RNIS

4.1.6 Détermination de l'interface RNIS du routeur

Aux États-Unis, c'est au client qu'il incombe de fournir la NT1. En Europe et dans d'autres pays, la compagnie téléphonique fournit la fonction NT1 et présente une interface S/T au client. Avec ces configurations, le client n'est pas tenu de fournir une unité NT1 distincte, ni une fonction NT1 intégrée à l'équipement terminal. Les équipements tels que les modules et interfaces RNIS d'un routeur doivent être commandés en conséquence. [1]



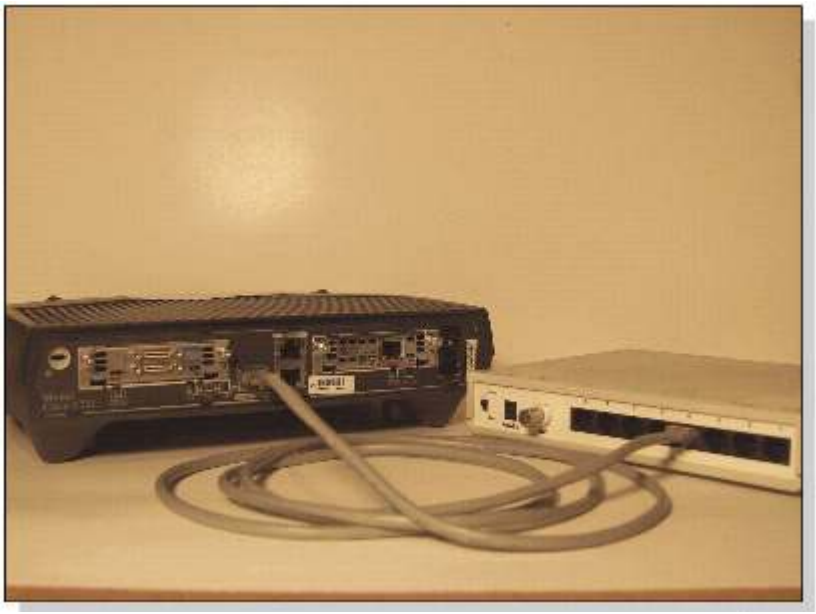
Avantages :

1. Routeur Cisco 2620 avec interface RNIS S/T (utilisé dans des installations RNIS non américaines)
2. Routeur Cisco 2620 avec interface RNIS U (utilisé dans des installations RNIS américaines)

Pour sélectionner un routeur Cisco avec l'interface RNIS appropriée, procédez comme suit:

1. Déterminez si le routeur prend en charge RNIS BRI. Recherchez un connecteur BRI ou une carte d'interface BRI WAN (WIC) à l'arrière du routeur.
2. Déterminez le fournisseur de la NT1. Une NT1 termine la boucle locale vers le central téléphonique (CO) du fournisseur d'accès RNIS. Aux États-Unis, la NT1 fait partie des équipements placés chez le client pour l'opérateur (CPE), à savoir que c'est le client qui en est responsable. En Europe, l'opérateur fournit généralement la NT1.
3. Si la NT1 est intégrée au CPE, le routeur doit avoir une interface U. Si le routeur est équipé d'une interface S/T, il nécessite alors une NT1 externe pour se connecter au fournisseur RNIS. 2

4. Si le routeur est doté d'un connecteur libellé BRI, il est déjà compatible RNIS. Avec une interface RNIS native déjà intégrée, le routeur est un TE1 et doit se connecter à une NT1. Si le routeur a une interface U, il dispose également d'une NT1 intégrée. 3



Si le routeur ne comporte aucun connecteur BRI et qu'il s'agit d'un routeur à configuration fixe ou non modulaire, il doit alors utiliser une interface série existante. Avec les interfaces RNIS non natives, telles que les interfaces série, un adaptateur de terminal externe doit être relié à l'interface série pour fournir la connectivité BRI. Si le routeur est modulaire, il peut être possible d'effectuer une mise à niveau vers une interface RNIS native, à condition qu'un emplacement soit disponible.

ATTENTION:

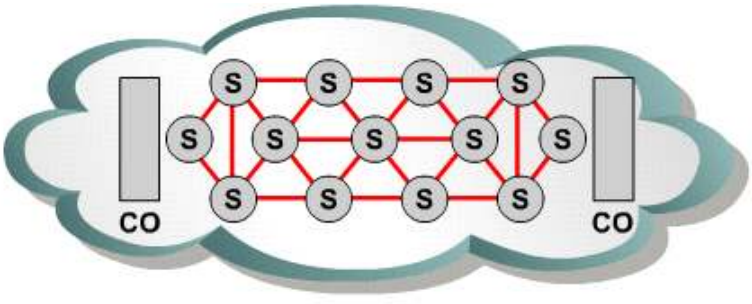
Ne connectez jamais un routeur avec interface U à une NT1, au risque d'endommager l'interface.

4.1 Concepts RNIS

4.1.7 Types de commutateurs RNIS

Les routeurs doivent être configurés pour identifier le type de commutateur avec lequel ils vont communiquer. Les types de commutateurs RNIS varient, partiellement en fonction du pays dans lequel le commutateur est utilisé. En conséquence des diverses mises en œuvre de la norme Q.931, le protocole de signalisation du canal D utilisé sur les commutateurs RNIS varie d'un constructeur à l'autre.

Les services offerts par les opérateurs RNIS varient considérablement d'un pays à l'autre et d'une région à l'autre. 1



De nombreux fournisseurs et types de commutateurs

Les services disponibles varient selon les régions et les pays

Comme c'est le cas pour les modems, chaque type de commutateur fonctionne de façon légèrement différente et comporte des exigences précises quant à l'établissement des appels. Avant que le routeur ne puisse être connecté à un service RNIS, il doit être configuré pour le type de commutateur utilisé au central téléphonique. Ces informations doivent être spécifiées au cours de la configuration du routeur, de manière à permettre à celui-ci de communiquer avec le commutateur, d'effectuer des appels RNIS au niveau réseau et d'envoyer des données. 2

Pays	Type de commutateur
États-Unis et Canada	AT&T 5ESS et 4ESS ; Northern Telecom DMS-100
France	VN2, VN3
Japon	NTT
Royaume-Uni	Net3 et Net5
Europe	Net3

Outre le type de commutateur utilisé par le fournisseur d'accès, il peut également s'avérer nécessaire de connaître les identificateurs de profil de service (SPID – *service profile identifiers*) attribués par l'opérateur téléphonique. Un SPID est un numéro fourni par l'opérateur RNIS permettant d'identifier la configuration de ligne du service BRI. Grâce aux identificateurs de profil de service (SPID), plusieurs unités RNIS, telles que des équipements voix et données, peuvent partager la boucle locale. Les SPID sont requis par les commutateurs DMS-100 et National ISDN-1.

Les SPID sont utilisés en Amérique du Nord et au Japon uniquement. L'opérateur RNIS fournit cet identificateur afin de déterminer la configuration de ligne du service RNIS. Dans de nombreux cas, les SPID doivent être entrés pendant la configuration d'un routeur.

Chaque SPID comporte des informations sur la configuration et l'établissement de la liaison. Les SPID sont des séries de caractères ressemblant généralement à des numéros de téléphone. Les SPID identifient chaque canal B pour le commutateur situé au central téléphonique. Une fois identifié, le commutateur relie les services disponibles à la connexion. N'oubliez pas que la technologie RNIS est généralement utilisée pour établir une connexion à accès commuté. Les SPID sont traités au moment de la connexion initiale du routeur au commutateur RNIS. Si des SPID sont requis mais qu'ils ne sont pas configurés correctement, l'initialisation échoue et les services RNIS ne peuvent pas être utilisés.

4.2 Configuration RNIS

4.2.1 Configuration de RNIS BRI

La commande **`isdn switch-type switch-type`** peut être configurée dans le mode de commande global ou d'interface afin de spécifier le commutateur RNIS du fournisseur. 1

Étape 1 : définition du type de commutateur RNIS

```
Router(config)#isdn switch-type switch-type
```

```
Router(config-if)#isdn switch-type switch-type
```

Indique le type de commutateur RNIS avec lequel le routeur communique

Certains fournisseurs peuvent formuler des exigences différentes en matière de configuration

Le fait de configurer la commande **`isdn switch-type`** en mode de configuration globale définit le type de commutateur RNIS de façon identique pour toutes les interfaces RNIS. Il est possible de configurer individuellement certaines interfaces à la suite de la commande de configuration globale, afin de refléter un type différent de commutateur.

À l'installation du service RNIS, l'opérateur fournit des informations sur le type de commutateur et les SPID. Les SPID servent à définir les services à la disposition des abonnés RNIS individuels. En fonction du type de commutateur, ces SPID peuvent devoir

être ajoutés à la configuration. Les commutateurs RNIS National ISDN-1 et DMS-100 ISDN nécessitent que des SPID soient configurés, mais ce n'est pas le cas du AT&T 5ESS. Des SPID doivent être spécifiés avec le simulateur RNIS Adtran.

Le format des SPID varie en fonction du type de commutateur RNIS et de certaines conditions spécifiques du fournisseur. Utilisez les commandes du mode de configuration d'interface **isdn spid1** et **isdn spid2** pour spécifier le SPID requis par le réseau RNIS quand le routeur établit une connexion vers l'échange RNIS local. 2 – 3

Étape 2 : (facultatif) configuration des numéros SPID

```
Router(config-if)#isdn spid1 spid-number [ldn]
```

Définit le numéro SPID attribué au canal B1 par le fournisseur d'accès RNIS.

```
Router(config-if)#isdn spid2 spid-number [ldn]
```

Définit le numéro SPID attribué au canal B2 par le fournisseur d'accès RNIS.

Paramètres des commandes isdn spid1 et isdn spid2	Description
spid-number	Numéro d'identification du service auquel a souscrit l'abonné. Cette valeur est attribuée par le fournisseur d'accès RNIS.
ldn	Numéro local. Sur la plupart des commutateurs, ce numéro doit correspondre aux informations relatives au destinataire (lesquelles proviennent du commutateur RNIS) pour qu'il soit possible d'utiliser les deux canaux B. Ce paramètre est facultatif.

La configuration de RNIS BRI est un mélange de commandes globales et d'interface. 4

Cisco

```
isdn switch-type basic-ni
!
<Output Omitted>
!
interface BRI0/0
 isdn switch-type basic-ni
 isdn spid1 51055540000001 5554000
 isdn spid2 51055540010001 5554001
!
```

Pour configurer le type de commutateur RNIS, utilisez la commande **isdn switch-type** en mode de configuration globale:

```
Router(config)#isdn switch-type switch-type
```

L'argument *switch-type* indique le type de commutateur de l'opérateur. Pour désactiver le commutateur sur l'interface RNIS, spécifiez **isdn switch-type none**. L'exemple suivant configure le type de commutateur National ISDN-1 en mode de configuration globale:

```
Router(config)#isdn switch-type basic-ni
```

Pour définir les SPID, utilisez la commande isdn spid# en mode de configuration d'interface. Cette commande permet de définir les numéros de SPID qui ont été attribués pour les canaux B:

```
Router(config-if)#isdn spid1 spid-number [ldn]
Router(config-if)#isdn spid2 spid-number [ldn]
```

L'argument facultatif **ldn** définit un numéro d'annuaire local. Sur la plupart des commutateurs, le numéro doit concorder avec les informations relatives à l'appelé provenant du commutateur RNIS. Les SPID se spécifient en mode de configuration d'interface. Pour passer en mode de configuration d'interface, utilisez la commande **interface bri** en mode de configuration globale:

```
Router(config)#interface bri slot/port
Router(config)#interface bri0/0
Router(config-if)#isdn spid1 51055540000001 5554000
Router(config-if)#isdn spid2 51055540010001 5554001
```

Activité de TP

Exercice: Configuration de l'interface RNIS BRI (interface U)

Au cours de ce TP, l'étudiant va configurer un routeur RNIS afin d'établir une connexion vers un commutateur RNIS local.

4.2 Configuration RNIS

4.2.2 Configuration de RNIS PRI

Le RNIS PRI est fourni sur une ligne louée T1 ou E1. Les principales tâches de configuration de PRI sont présentées ci-dessous:

Étape 1 : définition du type de commutateur RNIS

```
Router(config)#isdn switch-type switch-type
```

Étape 2 : sélection du contrôleur

```
Router(config)#controller controller slot/port
```

Étape 3 : définition du port d'interface de sorte qu'il fonctionne comme PRI

```
Router(config-controller)#pri-group timeslots range
```

1

1. Spécifiez le type de commutateur PRI avec lequel le routeur assure l'interface au central téléphonique de l'opérateur RNIS.
2. Spécifiez le contrôleur T1/E1, le type de tramage et le codage de ligne de l'installation de l'opérateur RNIS.
3. Définissez un groupe de tranches de temps PRI pour l'installation T1/E1 et indiquez la vitesse utilisée.

Comme les routeurs se connectent à PRI au moyen d'une ligne T1/E1, aucune commande «**interface pri**» ne s'avère nécessaire. Au lieu de cela, l'interface physique du routeur qui se connecte à la ligne louée est appelée contrôleur T1, ou contrôleur E1 dans le cas d'une ligne E1. Ce contrôleur doit être configuré correctement pour communiquer avec le réseau de l'opérateur. Les canaux RNIS PRI D et PRI B se configurent séparément à partir du contrôleur, au moyen de la commande **interface serial**.

Utilisez la commande **isdn switch-type** pour spécifier le commutateur RNIS utilisé par le fournisseur chez lequel le PRI se connecte. Comme avec BRI, cette commande peut être exécutée de façon globale ou en mode de configuration d'interface. Le tableau présente les types de commutateurs disponibles pour une configuration RNIS PRI: 2

Type de commutateur	Description
primaire-5ess	Commutateurs d'accès de base AT&T (États-Unis)
primaire-dms100	Northern Telecom DMS-100 (Amérique du Nord)
primaire-ni	National ISDN (Amérique du Nord)
primaire-net5	Type de commutateur pour Net5 au Royaume-Uni, en Europe et en Australie
primaire-ntt	Commutateur RNIS NTT (Japon)

```
Router(config)#isdn switch-type primary-net5
```

La configuration d'un contrôleur T1 ou E1 s'effectue en quatre étapes:

T1 - Exemple de configuration

```
Router(config)#controller t1 1/0
Router(config-controller)#framing esf
Router(config-controller)#linecode b8zs
Router(config-controller)#pri-group timeslots 1-24

Router(config-controller)#interface serial1/0:23
Router(config-if)#isdn switch-type primary-5ess
Router(config-if)#no cdp enable
```

E1 - Exemple de configuration

```
Router(config)#controller e1 1/0
Router(config-controller)#framing crc4
Router(config-controller)#linecode hdb3
Router(config-controller)#pri-group timeslots 1-31

Router(config-controller)#interface serial1/0:15
Router(config-if)#isdn switch-type primary-net5
Router(config-if)#no cdp enable
```

1. En mode de configuration globale, indiquez le contrôleur et l'emplacement/port du routeur dans lequel la carte PRI réside:

   ```
   Router(config)#controller {t1 | e1} {slot/port}
   Router(config-controller)#
   ```

2. Configurez le tramage, le codage de ligne et la synchronisation selon les spécifications de l'opérateur. La commande **framing** permet de sélectionner le type de trame utilisé par le fournisseur PRI. Pour T1, utilisez la syntaxe ci-dessous:

   ```
   Router(config-controller)#framing {sf | esf}
   ```

   Pour des lignes E1, utilisez la commande **framing** avec les options suivantes:

   ```
   Router(config-controller)#framing {crc4 | no-crc4} [australia]
   ```

   Utilisez la commande **linecode** pour identifier la méthode de signalisation de couche physique de l'installation numérique du fournisseur:

   ```
   Router(config-controller)#linecode {ami | b8zs| hdb3}
   ```

En Amérique du Nord, la méthode de signalisation B8ZS est utilisée pour les installations d'opérateurs T1. Elle permet d'utiliser l'intégralité des 64 kbits/s sur chaque canal RNIS. En Europe, c'est généralement le codage HDB3 qui est employé.

3. Configurez l'interface spécifiée pour l'accès PRI et le nombre de tranches de temps fixes allouées sur l'installation numérique du fournisseur:

```
Router(config-controller)#pri-group [timeslots range]
```

Pour T1, la plage de tranches de temps s'étend de 1 à 24. Pour E1, cette plage est de 1 à 31.

4. Spécifiez une interface pour le fonctionnement du canal D de l'accès PRI. Il s'agit d'une interface série vers une ligne T1/E1 sur le routeur:

```
Router(config)#interface serial{slot/port: | unit:}{23 | 15}
```

Au sein d'une installation E1 ou T1, la numérotation des canaux commence à 1. La numérotation varie de 1 à 31 pour E1 et de 1 à 24 pour T1. La numérotation des interfaces série sur les routeurs Cisco commence à 0. Par conséquent, le canal 16, à savoir le canal de signalisation E1, est le canal 15 de l'interface. Le canal 24, c'est-à-dire le canal de signalisation T1, devient le canal 23 sur l'interface. Ainsi, l'interface série 0/0:23 désigne le canal D d'un PRI T1.

Les sous-interfaces, couramment utilisées avec Frame Relay, sont désignées par un point. Par exemple, série 0/0.16 représente une sous-interface. Ne confondez pas les canaux d'une ligne T1 ou E1 avec des sous-interfaces. En effet, les canaux utilisent le caractère deux-points (:) au lieu du point pour désigner le numéro de canal:

- S0/0.23 désigne une sous-interface.
- S0/0:23 désigne un canal.

Activité de TP

Activité en ligne: isdn switch-type

Au cours de cette activité, l'étudiant va apprendre comment utiliser la commande **isdn switch-type**.

4.2 Configuration RNIS

4.2.3 Vérification de la configuration RNIS

Il est possible d'utiliser plusieurs commandes **show** pour vérifier que la configuration RNIS a été mise en œuvre correctement. 1

Affiche l'état d'une connexion RNIS

```
Router#show isdn status
```

Affiche des statistiques relatives à l'interface BRI configurée sur le routeur

```
Router#show interface bri0/0
```

Affiche des informations sur la communication en cours

```
Router#show isdn active
```

Pour confirmer le fonctionnement de l'accès BRI, utilisez la commande **show isdn status** pour inspecter l'état des interfaces BRI. Cette commande peut être utilisée après la configuration du RNIS BRI afin de vérifier que l'équipement terminal

TE1, ou le routeur, communique correctement avec le commutateur RNIS. Dans les résultats renvoyés en figure 2, la négociation des identificateurs de point d'extrémité de terminal (TEI) a réussi et la couche 3 RNIS est prête à effectuer ou à recevoir des appels.

Cisco

```
Cork#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
ACTIVE
    Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
TEI = 65, Ces = 2, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
TEI 64, ces = 1, state = 5(init)
    spid1 configured, no LDN, spid1 sent, spid1 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 1
TEI 65, ces = 2, state = 5(init)
    spid2 configured, no LDN, spid2 sent, spid2 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 2
    Layer 3 Status:
```

Assurez-vous que la couche 1 présente l'état ACTIVE, et la couche 2, l'état MULTIPLE_FRAME_ESTABLISHED. Cette commande présente également le nombre de communications actives.

La commande **`show isdn active`** affiche des informations sur l'appel en cours, notamment les suivantes:

- Le numéro appelé
- La durée de l'appel avant déconnexion
- L'indication du coût
- Les unités de facturation utilisées pendant l'appel
- Le fait que les informations d'indication du coût soient fournies pendant ou à la fin des appels

La commande **`show dialer`** présente des informations sur l'interface de numérotation:

- L'état de la communication en cours
- Les valeurs de l'horloge de ligne téléphonique
- La raison de l'appel
- L'équipement distant connecté

La commande **`show interface bri0/0`** affiche des statistiques relatives à l'interface BRI configurée sur le routeur. Des informations spécifiques du canal sont renvoyées lorsque vous placez le numéro du canal à la fin de la commande. Dans ce cas, la commande **`show interface bri0/0:1`** renvoie les informations suivantes:

- Le canal B utilise l'encapsulation PPP.
- La trame LCP a été négociée et est ouverte.
- Il y a deux protocoles de contrôle NCP actifs, à savoir IPCP et CDPCP (*Cisco Discovery Protocol Control Protocol*). 3

Cisco

```
BranchF#show interface bri0/0:1
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set
(10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:01, output 00:00:01, output hang
never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output
drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max
```

Activité de TP

Activité en ligne: show isdn status

Au cours de cette activité, l'étudiant va apprendre comment utiliser la commande **show isdn status** pour afficher l'état de toutes les interfaces RNIS.

4.2 Configuration RNIS

4.2.4 Dépannage de la configuration RNIS

Les commandes suivantes servent à déboguer et à dépanner la configuration RNIS: 1

- La commande **debug isdn q921** montre les messages de la couche de liaison de données, dite couche 2, sur le canal D entre le routeur et le commutateur RNIS. Utilisez cette commande si **show isdn status** ne renvoie pas ACTIVE pour la couche 1 et MULTIPLE_FRAME_ESTABLISHED pour la couche 2.
- La commande **debug isdn q931** montre l'échange de messages d'établissement et d'interruption de communication de la connexion RNIS de couche 3.
- La commande **debug ppp authentication** affiche les messages du protocole d'authentification PPP, notamment les échanges CHAP (*Challenge Handshake Authentication Protocol*) et PAP (*Password Authentication Protocol*).
- La commande **debug ppp negotiation** affiche des informations sur le trafic et les échanges PPP pendant la négociation des composants PPP. Ceci inclut les échanges LCP, d'authentification et NCP. Une négociation PPP réussie ouvre tout d'abord l'état LCP, puis procède à l'authentification, pour terminer par la négociation de NCP.
- La commande **debug ppp error** affiche les erreurs de protocole et les statistiques d'erreur associées à la négociation et à l'utilisation de la connexion PPP. Utilisez les commandes **debug ppp** pour résoudre un problème de couche 2 si la commande **show isdn status** n'indique aucun problème du RNIS.

```
Router#debug isdn q921
```

Affiche les messages de la couche 2 RNIS

```
Router#debug isdn q931
```

Affiche l'activité d'établissement et d'interruption de communication RNIS de la couche 3

```
Router#debug ppp authentication
```

Affiche les messages du protocole d'authentification PPP

```
Router#debug ppp negotiation
```

Affiche les informations relatives à l'établissement de la liaison PPP

```
Router#debug ppp error
```

Affiche des erreurs de protocole associées au protocole PPP

4.3 Configuration DDR

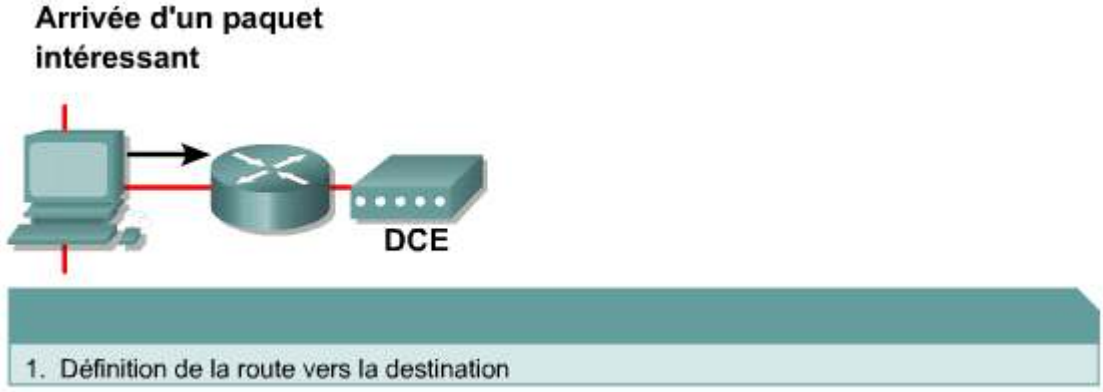
4.3.1 Fonctionnement de DDR

Le routage à établissement de connexion à la demande (DDR – *Dial-on-demand routing*) se déclenche quand du trafic concordant avec un ensemble de critères prédéfini est mis en file d'attente pour être envoyé sur une interface compatible DDR. Le trafic qui occasionne un appel DDR est appelé trafic intéressant. Une fois que le routeur a transmis le trafic intéressant, la communication prend fin.

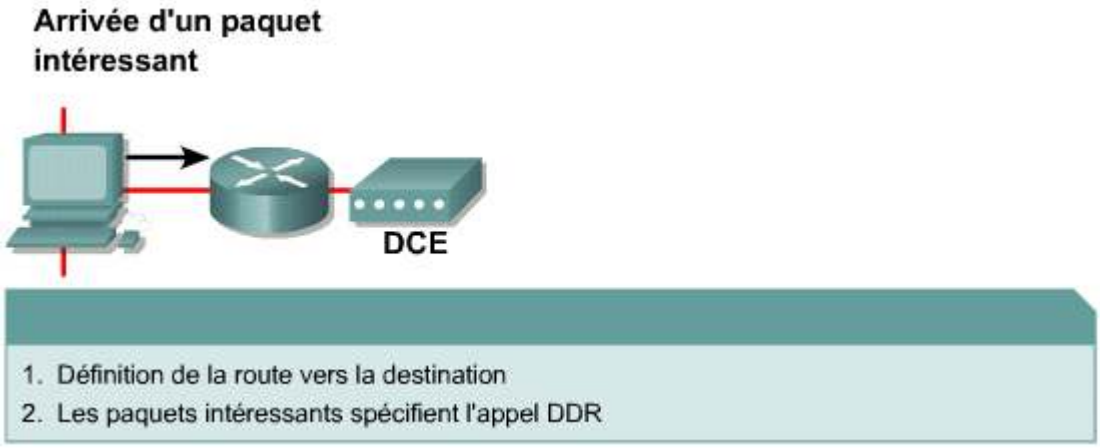
La définition du trafic intéressant constitue la clé de l'efficacité de DDR. Le trafic intéressant se définit au moyen de la commande **`dialer-list`**. Les listes de numérotation peuvent autoriser tout le trafic d'un protocole spécifique à établir une liaison DDR, ou peuvent interroger une liste d'accès pour déterminer les types de trafics spécifiques pouvant établir la liaison. Les listes de numérotation ne filtrent pas le trafic sur une interface. Même le trafic qui n'est pas intéressant est transféré si la connexion vers la destination est active.

La procédure ci-dessous permet de mettre en œuvre DDR sur les routeurs Cisco:

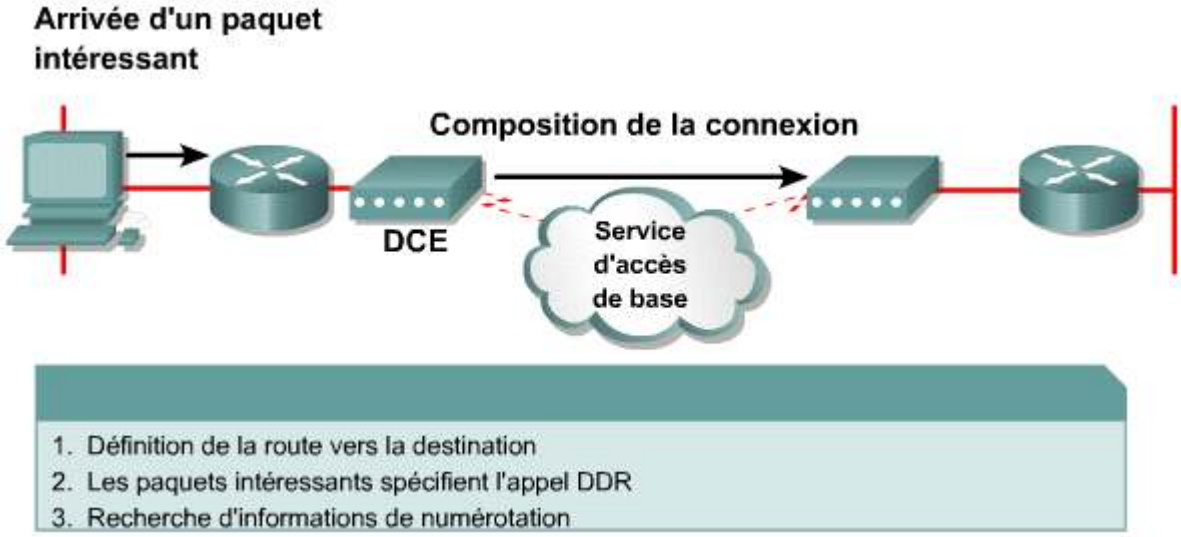
1. Le routeur reçoit du trafic, interroge une table de routage afin de déterminer s'il existe une route vers la destination, puis identifie l'interface sortante. 1



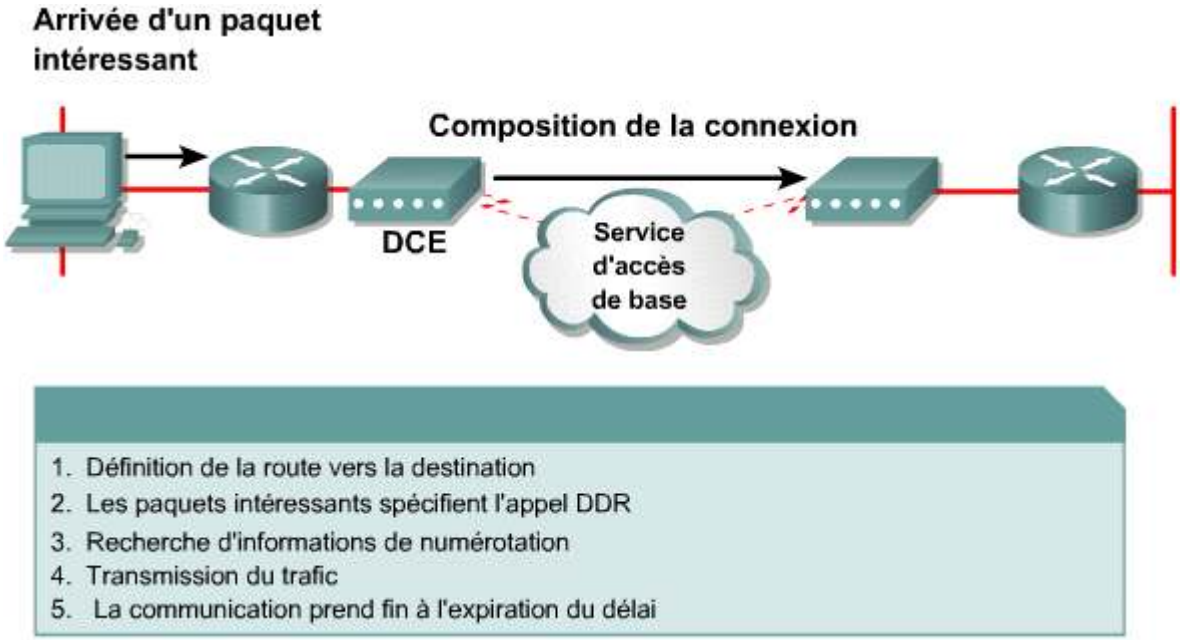
2. Si l'interface sortante est configurée pour DDR, le routeur effectue une interrogation pour déterminer si le trafic est intéressant. 2


Arrivée d'un paquet intéressant
DCE
1. Définition de la route vers la destination
2. Les paquets intéressants spécifient l'appel DDR

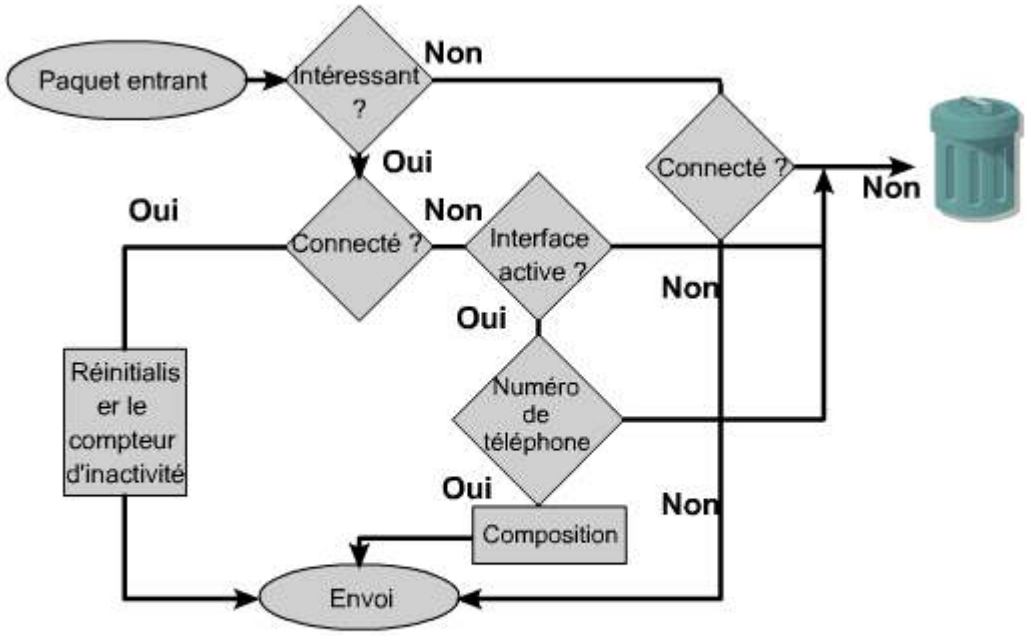
3. Le routeur identifie les informations de numérotation nécessaires pour effectuer l'appel en utilisant une carte de numérotation pour accéder au routeur du saut suivant. 3


Arrivée d'un paquet intéressant
Composition de la connexion
DCE
Service d'accès de base
1. Définition de la route vers la destination
2. Les paquets intéressants spécifient l'appel DDR
3. Recherche d'informations de numérotation

4. Le routeur vérifie ensuite si la carte de numérotation est en cours d'utilisation. Si l'interface est connectée à la destination distante souhaitée, le trafic est envoyé. Si l'interface n'est pas connectée à la destination distante, le routeur envoie des informations d'établissement d'appel par le canal D sur le BRI. 4


Arrivée d'un paquet intéressant
Composition de la connexion
DCE
Service d'accès de base
1. Définition de la route vers la destination
2. Les paquets intéressants spécifient l'appel DDR
3. Recherche d'informations de numérotation
4. Transmission du trafic
5. La communication prend fin à l'expiration du délai

5. Une fois la liaison établie, le routeur transmet le trafic intéressant et inintéressant. Le trafic inintéressant peut inclure des mises à jour de données et de routage.
6. Le compteur d'inactivité se déclenche et fonctionne tant qu'aucun trafic intéressant ne survient au cours de la période d'inactivité, puis déconnecte la communication en fonction de la manière dont elle est configurée. 5



Cet organigramme illustre comment un routeur détermine s'il y a lieu ou non d'initier une connexion DDR.

La configuration du compteur d'inactivité spécifie la durée pendant laquelle le routeur doit rester connecté si aucun trafic intéressant n'a été envoyé. Une fois qu'une connexion DDR a été établie, n'importe quel trafic est autorisé vers la destination. En revanche, seul le trafic intéressant réinitialise le compteur d'inactivité.

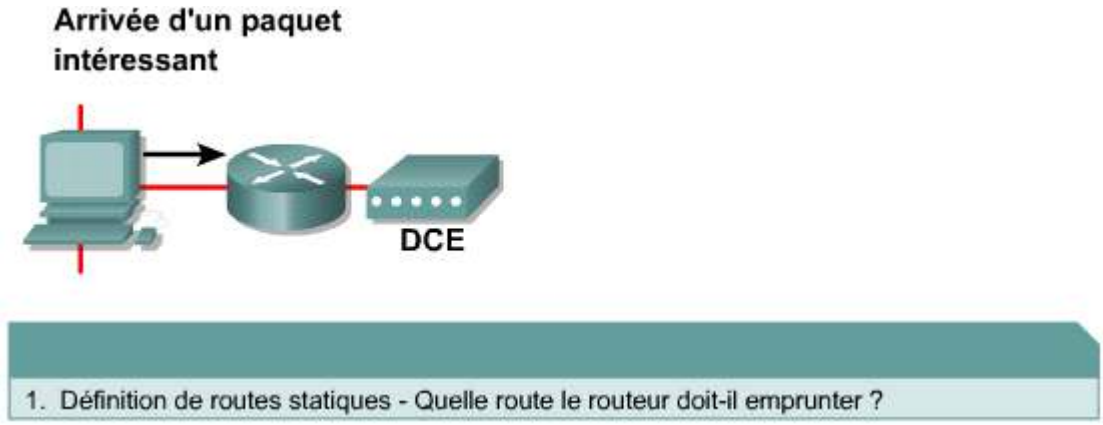
4.3 Configuration DDR

4.3.2 Configuration du DDR traditionnel

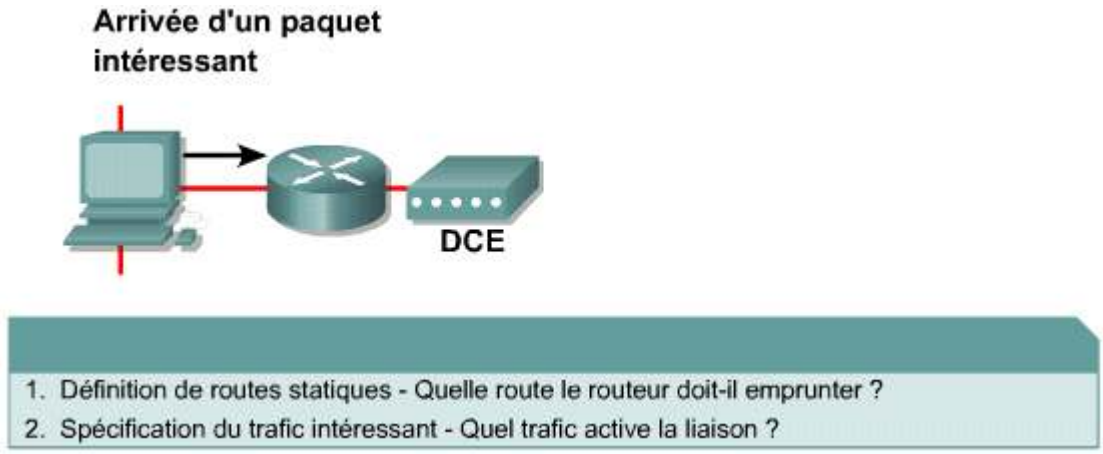
DDR traditionnel est un terme utilisé pour définir une configuration DDR élémentaire, avec laquelle un seul ensemble de paramètres de numérotation est appliqué à une interface. Si plusieurs configurations de numérotation sont requises sur une interface, il s'avère alors nécessaire d'utiliser des profils de numérotation.

Pour configurer le DDR traditionnel, procédez comme suit:

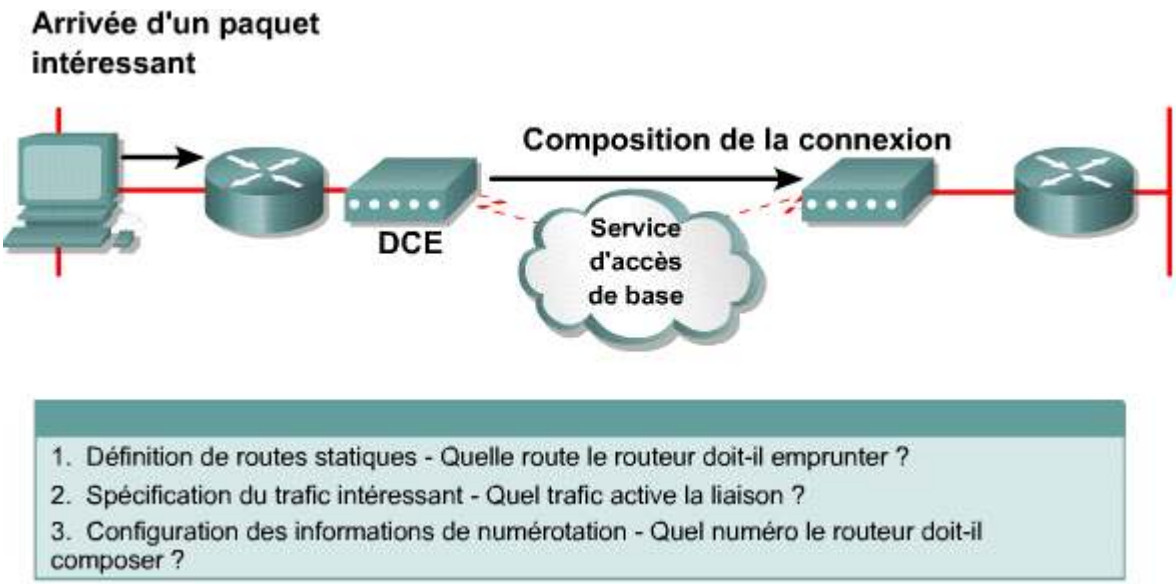
- Définissez des routes statiques. 1



- Spécifiez le trafic intéressant. 2


Arrivée d'un paquet intéressant
DCE
1. Définition de routes statiques - Quelle route le routeur doit-il emprunter ?
2. Spécification du trafic intéressant - Quel trafic active la liaison ?

- Configurez les informations de numérotation. 3


Arrivée d'un paquet intéressant
Composition de la connexion
DCE
Service d'accès de base
1. Définition de routes statiques - Quelle route le routeur doit-il emprunter ?
2. Spécification du trafic intéressant - Quel trafic active la liaison ?
3. Configuration des informations de numérotation - Quel numéro le routeur doit-il composer ?

Activité de TP

Exercice: Configuration du DDR traditionnel

Au cours de ce TP, l'étudiant va configurer un routeur RNIS pour effectuer un appel par routage à établissement de connexion à la demande (DDR – *dial-on-demand routing*) traditionnel vers un autre routeur compatible RNIS.

Pour transférer le trafic, les routeurs doivent connaître la route à utiliser pour une destination donnée. Quand un protocole de routage dynamique est utilisé, l'interface DDR appelle le site distant pour chaque mise à jour du routage ou message «hello» si ces paquets sont définis comme trafic intéressant. Pour éviter l'activation fréquente ou constante de la liaison DDR, configurez les routes nécessaires de façon statique.

Pour configurer une route statique pour IP, utilisez la commande ci-dessous:

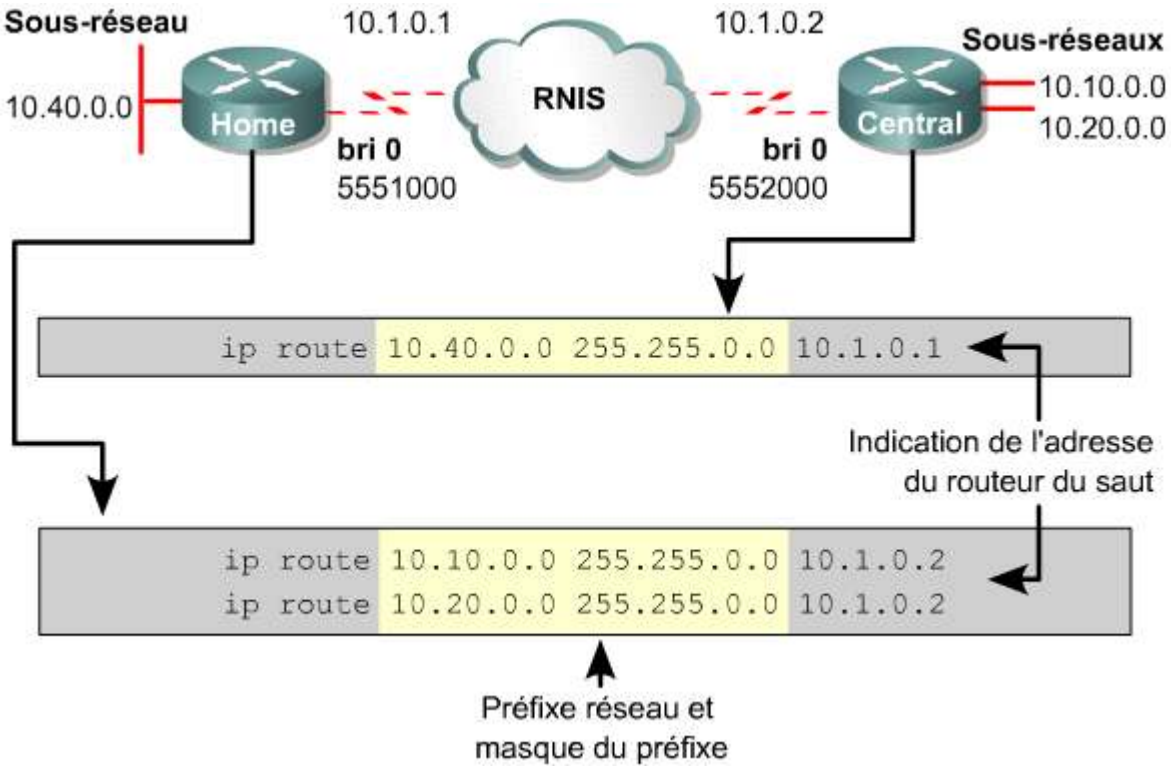
```
Router(config)#ip route net-prefix mask{address | interface} [distance] [permanent]
```

Le routeur Central dispose d'une route statique vers le réseau 10.40.0.0 sur le routeur Home. 1Le routeur Home dispose de deux routes statiques définies pour les deux sous-réseaux du réseau local Central. Si le réseau rattaché au routeur Home est un réseau d'extrémité, tout le trafic non local doit alors être envoyé vers Central. Une route par défaut constitue un meilleur choix pour le routeur Home dans ce cas précis.

```
Home(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.2
```

Lorsque vous configurez des routes statiques, tenez compte des facteurs ci-dessous:

- Par défaut, une route statique prend la priorité sur une route dynamique, du fait de sa distance administrative plus réduite. Sans configuration complémentaire, une route dynamique vers un réseau est ignorée s'il existe une route statique dans la table de routage pour le même réseau.
- Pour réduire le nombre d'entrées de routes statiques, définissez une route statique résumée ou par défaut.



4.3 Configuration DDR

4.3.4 Spécification du trafic intéressant pour DDR

Les communications DDR sont déclenchées par le trafic intéressant. Ce trafic peut correspondre à l'une des définitions ci-dessous:

- Le trafic IP d'un type de protocole particulier
- Les paquets avec une adresse source ou de destination particulière
- Les autres critères définis par l'administrateur réseau

Utilisez la commande **dialer-list** pour identifier le trafic intéressant. La syntaxe de cette commande est la suivante:

```
Router(config)#dialer-list dialer-group-numprotocolprotocol-name {permit | deny | list
access-list-number}
```

Le paramètre dialer-group-num est un nombre entier entre 1 et 10 qui identifie la liste de numérotation pour le routeur. La commande **dialer-list 1 protocol ip permit** permet à tout le trafic IP de déclencher un appel. [1] Au lieu d'autoriser tout le trafic IP, une liste de numérotation peut pointer sur une liste d'accès afin de spécifier exactement les types de trafics qui doivent activer la liaison. La référence à la liste d'accès 101 dans la liste de numérotation 2 empêche le trafic FTP et Telnet d'activer la liaison DDR. N'importe quel autre paquet IP est considéré comme intéressant et active donc la liaison DDR.

Sans liste d'accès

```
dialer-list 1 protocol ip permit
```

Tout trafic IP active la liaison

Avec listes d'accès (pour un contrôle accru)

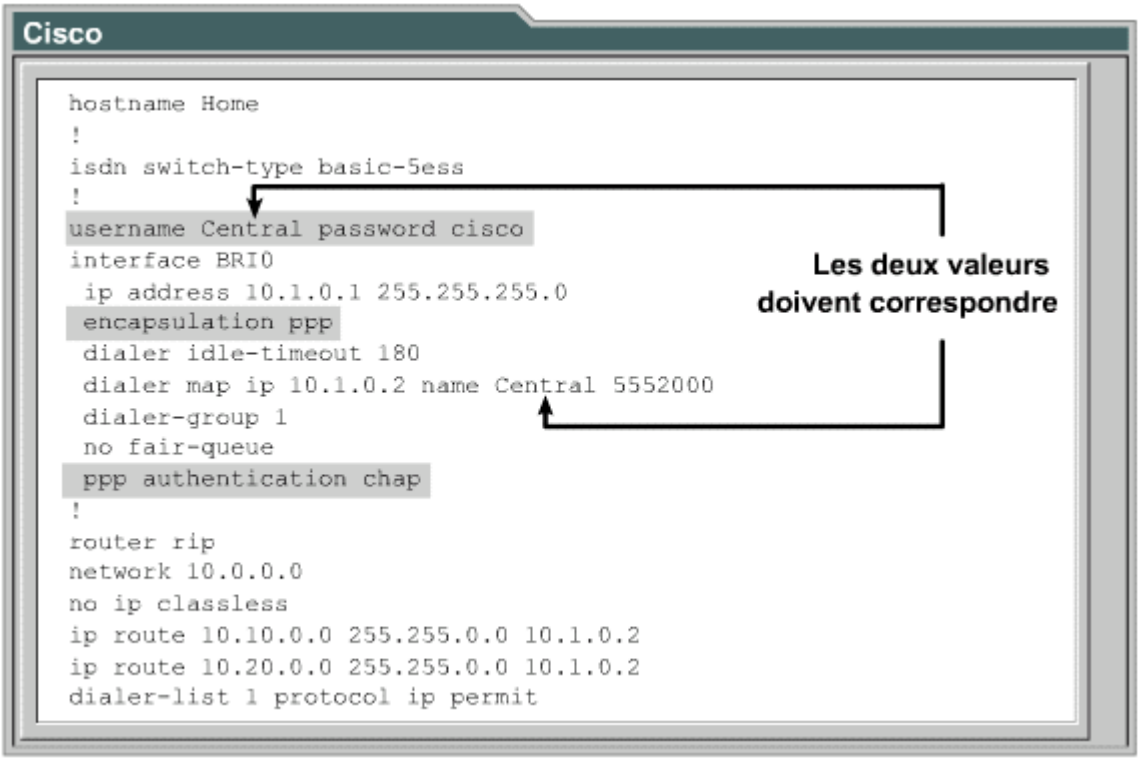
```
dialer-list 2 protocol ip list 101

access-list 101 deny tcp any any eq ftp      <-- Refuser FTP
access-list 101 deny tcp any any eq telnet   <-- Refuser Telnet
access-list 101 permit ip any any
```

Tout trafic IP active la liaison, à l'exception de FTP et Telnet

4.3 Configuration DDR

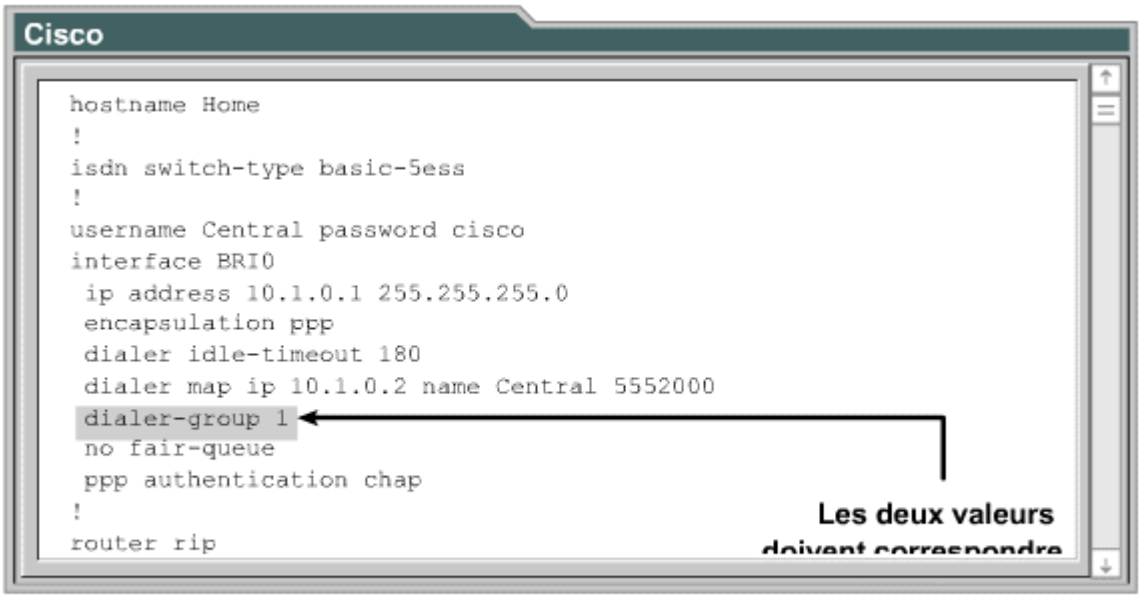
4.3.5 Configuration des informations de numérotation DDR

Plusieurs étapes interviennent dans la configuration de l'interface DDR. La configuration de PPP sur l'interface de numérotation s'effectue au moyen des mêmes commandes que celles qui activent PPP sur une interface série. HDLC constitue l'encapsulation par défaut pour une interface RNIS sur un routeur Cisco, mais la plupart des réseaux utilisent PPP pour les connexions à commutation de circuits. Du fait de sa robustesse, de son interopérabilité et de fonctionnalités supplémentaires, telles que l'authentification, PPP est le protocole de liaison de données utilisé sur les canaux B de la plupart des routeurs. Pour configurer PPP sur l'interface DDR, utilisez les commandes ci-dessous: [1]




```
Home(config)#username Central password cisco
Home(config)#interface bri0/0
Home(config-if)#encapsulation ppp
Home(config-if)#ppp authentication chap
Home(config-if)#ip address 10.1.0.1 255.255.255.0
```

Une liste de numérotation spécifiant le trafic intéressant pour cette interface DDR doit être associée à cette dernière. Pour ce faire, utilisez la commande **dialer-group group-number**:

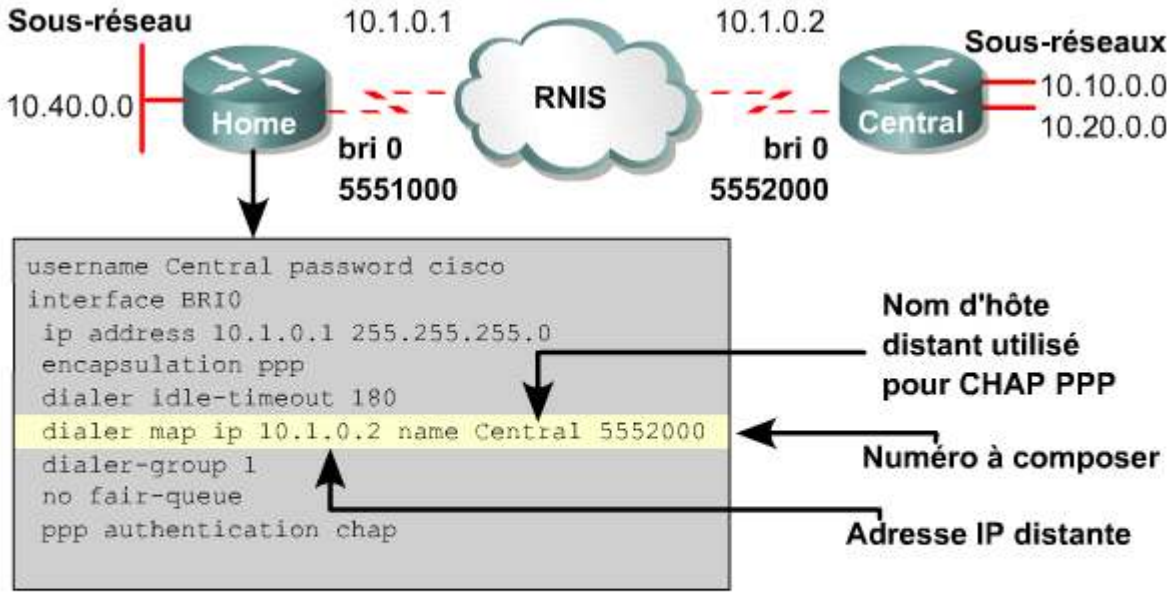


La commande dialer-group applique des règles définies par la liste de numérotation à des interfaces individuelles.

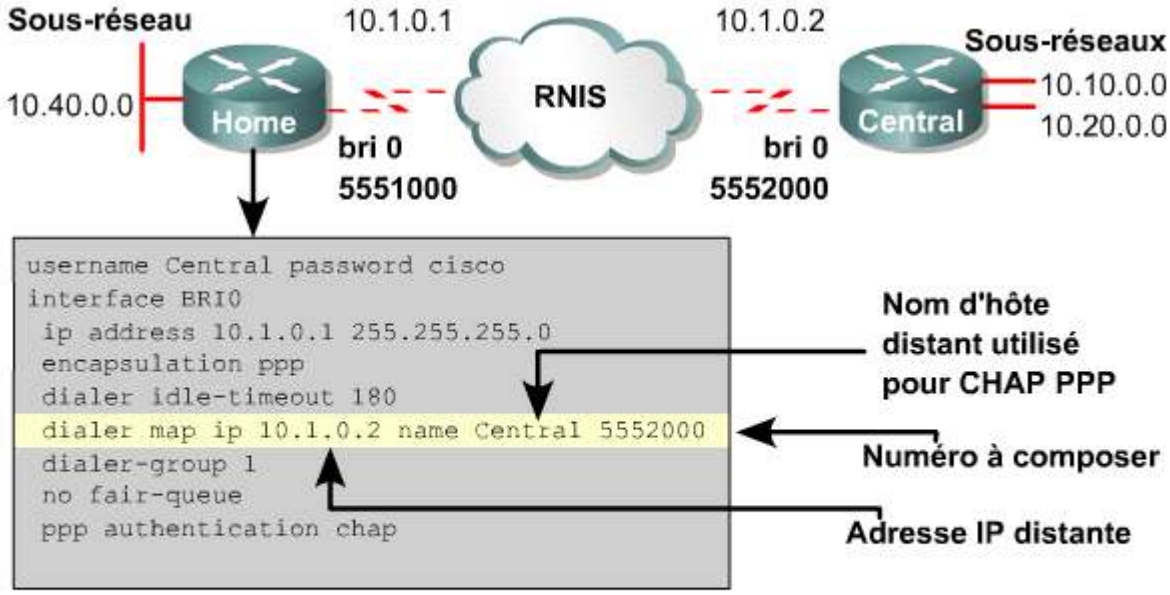
```
Home(config-if)#dialer-group 1
```

Dans la commande, **group-number** spécifie le numéro du groupe de numérotation auquel l'interface appartient. Le numéro du groupe peut être un nombre entier entre 1 et 10. Ce numéro doit concorder avec le **dialer-list group-number**. Chaque interface ne peut avoir qu'un groupe de numérotation. En revanche, la même liste de numérotation peut être attribuée à plusieurs interface à l'aide de la commande **dialer-group**.

Les informations de numérotation correctes pour l'interface DDR distante doivent être spécifiées. Pour ce faire, utilisez la commande **dialer map**: 3



Le paramètre de nom de la commande dialer map permet au routeur d'effectuer le suivi des appels RNIS en fonction du nom d'hôte du routeur distant.



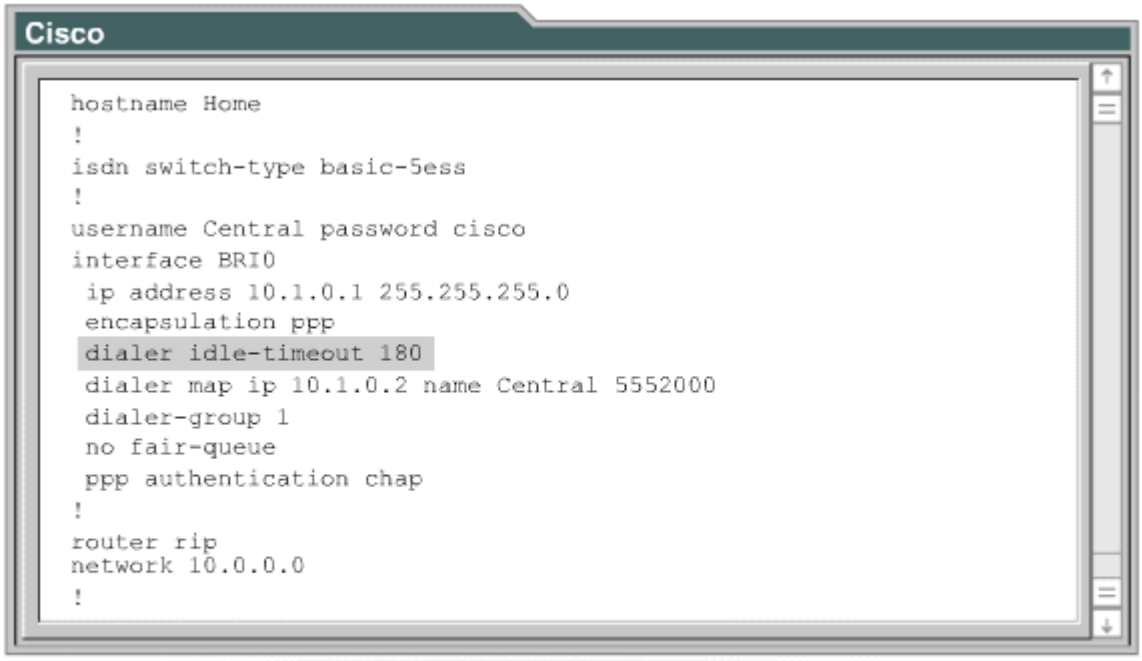
Le paramètre de nom de la commande dialer map permet au routeur d'effectuer le suivi des appels RNIS en fonction du nom d'hôte du routeur distant.

La commande dialer map mappe l'adresse du protocole distant sur un numéro de téléphone. Cette commande s'avère nécessaire pour appeler plusieurs sites.

```
Router(config-if)#dialer mapprotocol next-hop-address [namehostname] [speed 56 | 64]
[broadcast] dial-string
```

Si vous n'appelez qu'un site, utilisez une commande **dialer string** inconditionnelle qui appelle toujours ce numéro de téléphone unique, quelle que soit la destination du trafic. Cette étape est spécifique au DDR traditionnel. Bien que les informations soient toujours requises, les étapes de configuration des informations de destination sont différentes quand on utilise des profils de numérotation à la place du DDR traditionnel.

La commande **dialer idle-timeout seconds** peut être utilisée pour spécifier le nombre de secondes d'inactivité avant la déconnexion d'une communication. [4]



La commande dialer idle-timeout indique au routeur la durée d'activité de la connexion DDR si aucun trafic intéressant n'est envoyé.

Le paramètre **seconds** représente le nombre de secondes devant s'écouler avant la déconnexion de l'appel après l'envoi du dernier paquet intéressant. La valeur par défaut est de 120 secondes.

4.3 Configuration DDR

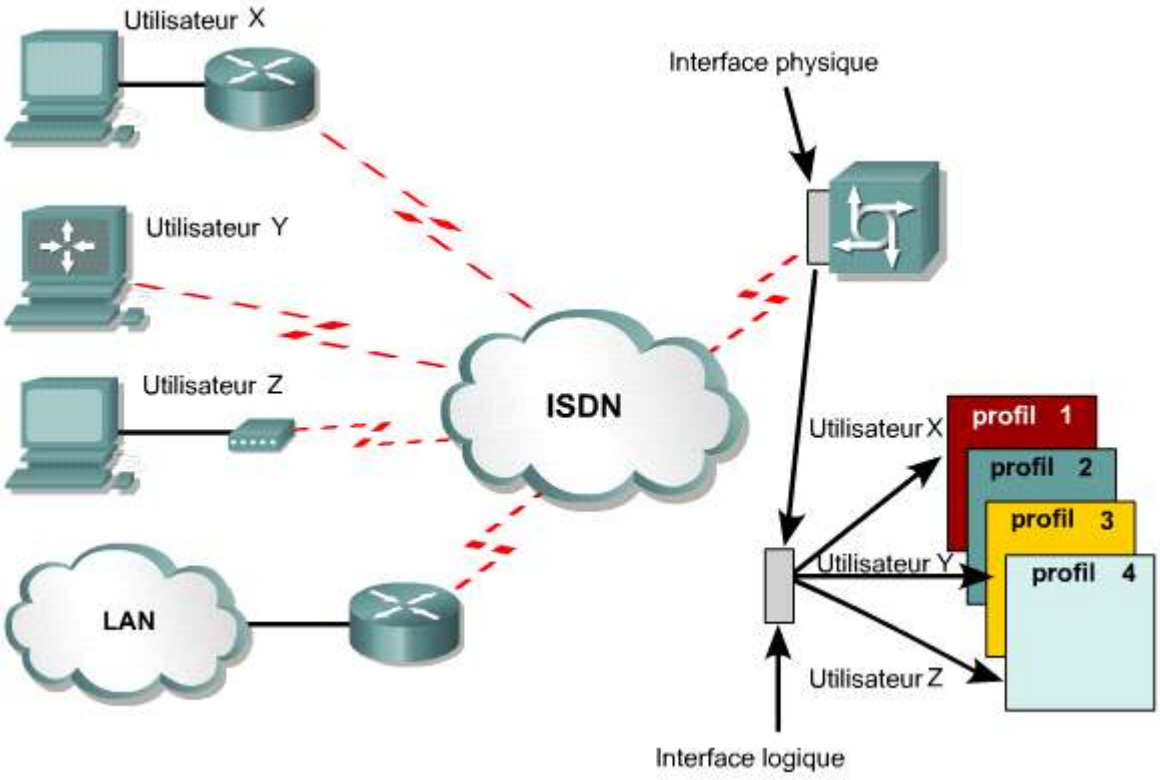
4.3.6 Profils de numérotation

Le DDR traditionnel est limité, car la configuration est appliquée directement à l'interface physique. Comme l'adresse IP est appliquée directement à l'interface, seules les interfaces DDR configurées dans ce sous-réseau spécifique peuvent établir une connexion DDR avec cette interface. Cela signifie qu'il existe une correspondance un pour un entre les deux interfaces DDR situées à chaque extrémité de la liaison.

Les profils de numérotation suppriment la configuration de l'interface qui reçoit ou effectue des appels et peuvent uniquement lier la configuration à l'interface appel par appel. Les profils de numérotation permettent à des interfaces physiques d'adopter de façon dynamique différentes caractéristiques, en fonction des conditions requises par l'appel entrant ou sortant. Les profils de numérotation peuvent effectuer les opérations suivantes:

- Définir l'encapsulation et les listes de contrôle d'accès
- Déterminer le nombre minimum ou maximum d'appels
- Activer ou désactiver les fonctions

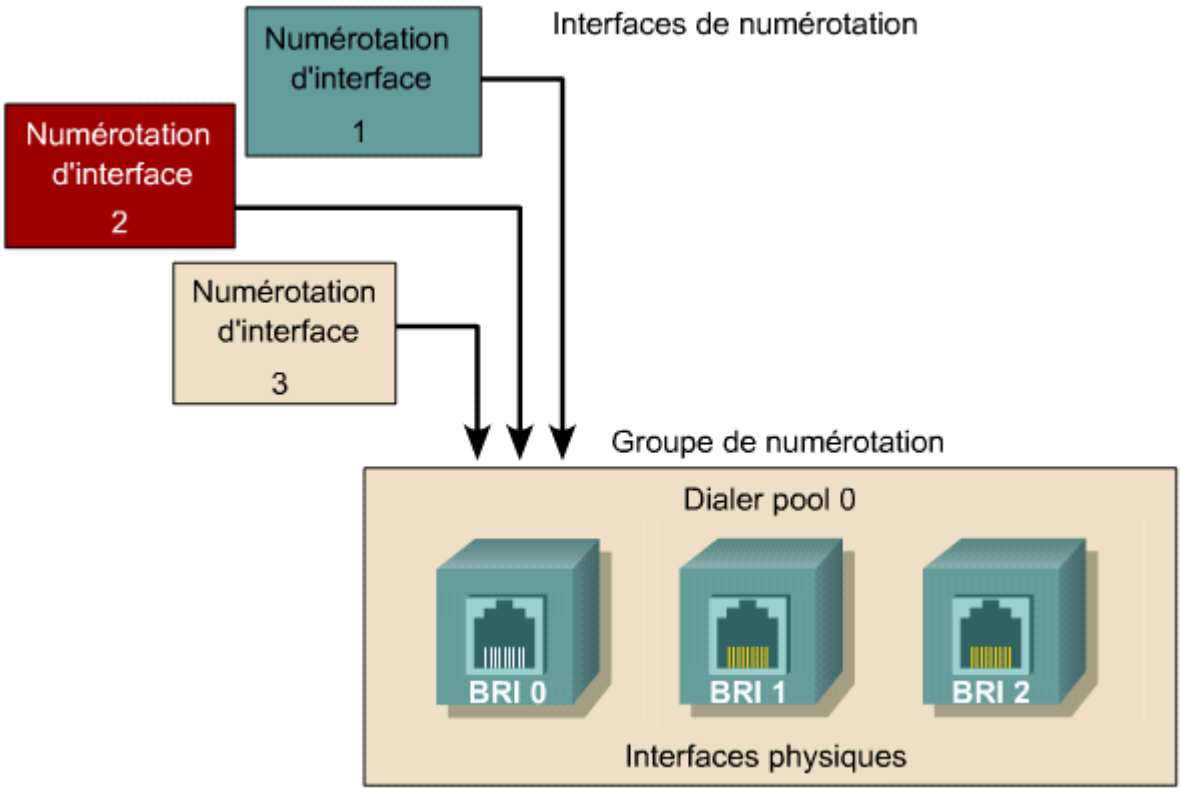
Les profils de numérotation facilitent la conception et le déploiement d'interréseaux à commutation de circuits plus complexes et plus évolutifs en mettant en œuvre un modèle DDR plus évolutif au niveau des routeurs Cisco et des serveurs d'accès. Les profils de numérotation séparent la partie logique de DDR, à savoir la couche réseau, l'encapsulation et les paramètres de numérotation, de l'interface physique qui émet ou reçoit les appels. [1]



Les profils de numérotation permettent d'effectuer les activités ci-dessous:

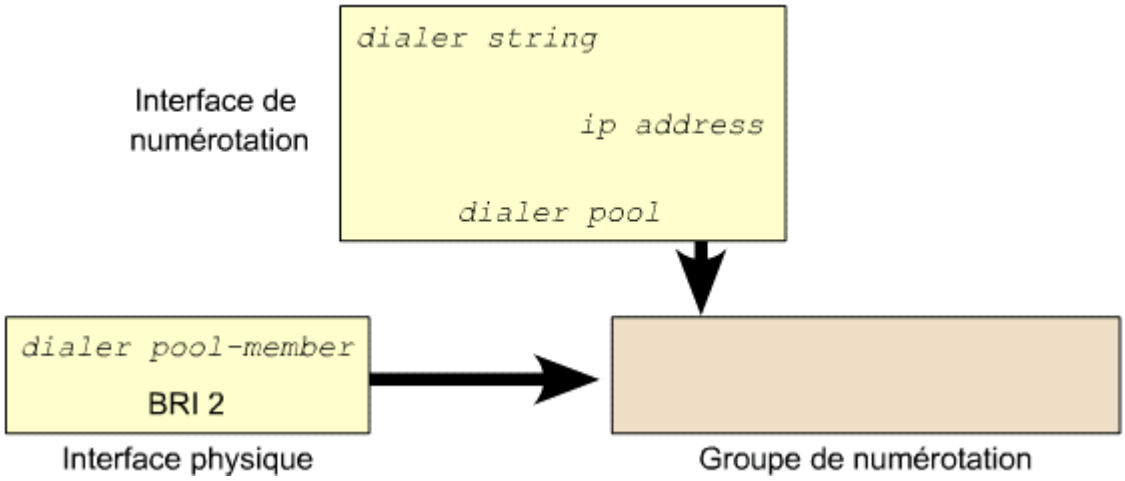
- Configurer les canaux B d'une interface RNIS avec différents sous-réseaux IP
- Utiliser différentes encapsulations sur les canaux B d'une interface RNIS
- Définir différents paramètres DDR pour les canaux B d'une interface RNIS
- Éliminer le gaspillage de canaux B RNIS en permettant aux accès RNIS BRI d'appartenir à plusieurs groupes de numérotation

Un profil de numérotation comporte les éléments suivants: 2



- **Interface de numérotation** – Entité logique qui utilise un profil de numérotation par destination.

- **Groupe de numérotation** – Chaque interface de numérotation désigne un groupe de numérotation, c'est-à-dire un groupe d'une ou plusieurs interfaces physiques associées à un profil de numérotation.
- **Interfaces physiques** – Les interfaces d'un groupe de numérotation sont configurées pour des paramètres d'encapsulation et pour identifier les groupes de numérotation auxquels l'interface appartient. L'authentification PPP, le type d'encapsulation et le PPP multiliaison sont tous configurés sur l'interface physique. 3



À l'instar du DDR traditionnel, les profils de numérotation s'activent quand du trafic intéressant est mis en fils d'attente en vue d'être envoyé vers une interface DDR. Tout d'abord, un paquet intéressant est routé vers une adresse IP DDR distante. Le routeur consulte ensuite les interfaces de numérotation configurées pour trouver celle qui partage le même sous-réseau que l'adresse IP DDR distante. S'il en existe une, le routeur recherche une interface DDR physique non utilisée dans le groupe de numérotation. La configuration du profil de numérotation est ensuite appliquée à l'interface, et le routeur tente de créer la connexion DDR. À la fin de la connexion, l'interface revient au groupe de numérotation pour l'appel suivant.

4.3 Configuration DDR

4.3.7 Configuration de profils de numérotation

Il est possible de configurer plusieurs interfaces de numérotation sur un routeur. Chaque interface constitue la configuration complète pour une destination. La commande **`interface dialer`** crée une interface de numérotation et passe en mode de configuration d'interface. 1

```
interface dialer1
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Smalluser
 dialer string 5554540
 dialer idle-timer 240
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
interface dialer2
 ip address 10.2.2.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Mediumuser
 dialer string 5551234
 dialer idle-timer 9999
 dialer pool 1
 dialer-group 2
```

Les profils de numérotation sont des interfaces logiques qui sont associées, de manière dynamique, à des interfaces physiques.

Pour configurer l'interface de numérotation, procédez comme suit:

1. Configurez une ou plusieurs interfaces de numérotation avec toutes les commandes DDR de base:
   - L'adresse IP
   - Le type d'encapsulation et l'authentification
   - Le compteur d'inactivité
   - Le groupe de numérotation pour le trafic intéressant
2. Configurez une **`dialer string`** et un **`dialer remote-name`** pour spécifier le nom du routeur distant et le numéro de téléphone permettant d'y accéder. La commande **`dialer pool`** associe cette interface logique avec un groupe d'interfaces physiques.
3. Configurez les interfaces physiques et assignez-les à un groupe de numérotation à l'aide de la commande **`dialer pool-member`**. 2

```
interface BRI0/0
 encapsulation ppp
 dialer pool-member 0 priority 100
 ppp authentication chap
!
interface BRI0/1
 encapsulation ppp
 dialer pool-member 1 priority 150
 ppp authentication chap
!
interface BRI0/2
 encapsulation ppp
 dialer pool-member 0 priority 50
 dialer pool-member 1 priority 50
 dialer pool-member 2 priority 50
 ppp authentication chap
!
```

Plusieurs groupes de numérotation peuvent être attribués à une interface au moyen de plusieurs commandes **`dialer pool-member`**. S'il existe plusieurs interfaces physiques dans le groupe, utilisez l'option **`priority`** de la commande **`dialer pool-member`** pour définir la priorité de l'interface au sein d'un groupe de numérotation. Si plusieurs appels doivent être effectués et qu'une seule interface est disponible, c'est le groupe qui a la priorité la plus élevée qui effectue l'appel.

Une combinaison de n'importe laquelle de ces interfaces peut être utilisée avec les groupes de numérotation:

- Série synchrone
- Série asynchrone
- BRI
- PRI

Activité de TP

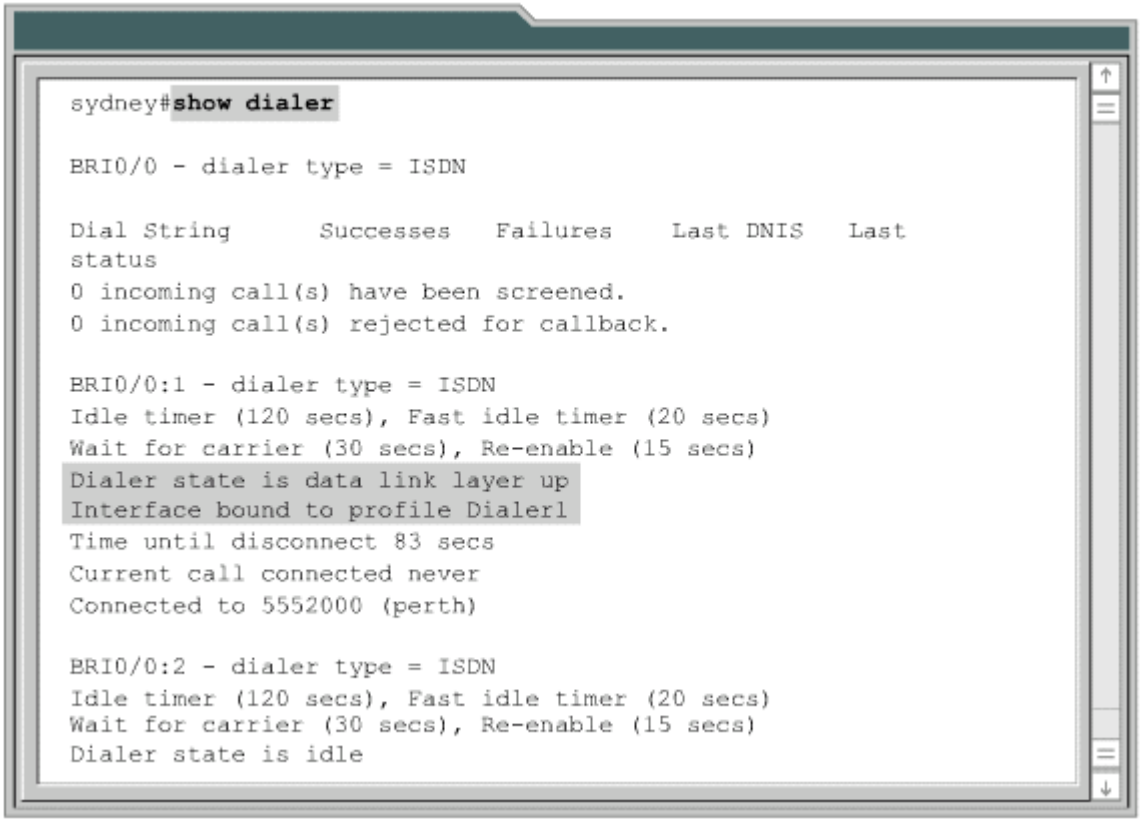
Exercice: Configuration de profils de numérotation

Au cours de ce TP, l'étudiant va configurer des profils de numérotation RNIS sur les routeurs.

4.3.8 Vérification de la configuration DDR

La commande **show dialer interface [BRI]** affiche des informations au même format que les statistiques du DDR traditionnel sur les appels entrants et sortants.

Le message «Dialer state is data link layer up» suggère que le numéroteur s'est activé correctement et que l'interface BRI 0/0:1 est liée au profil dialer1. 1


sydney#show dialer
BRI0/0 - dialer type = ISDN
Dial String Successes Failures Last DNIS Last
status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.
BRI0/0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Interface bound to profile Dialer1
Time until disconnect 83 secs
Current call connected never
Connected to 5552000 (perth)
BRI0/0:2 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle

La commande **show isdn active** présente des informations sur les communications RNIS actives en cours. 2 Dans cet écran, l'appel RNIS est sortant vers un routeur distant dénommé Seattle.

```
Phoenix#show isdn active
------------------------------------------------------------------------
-------------
                                ISDN ACTIVE CALLS
------------------------------------------------------------------------
-------------
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
------------------------------------------------------------------------
-------------
Call Calling Called  Remote Seconds Seconds Seconds Charges
Type Number  Number  Name   Used    Left    Idle    Units/Currency
------------------------------------------------------------------------
Out          5551000 Seattle      87      41      78      0
------------------------------------------------------------------------
```

La commande **show isdn status** présente des informations sur les trois couches de l'interface BRI. 3

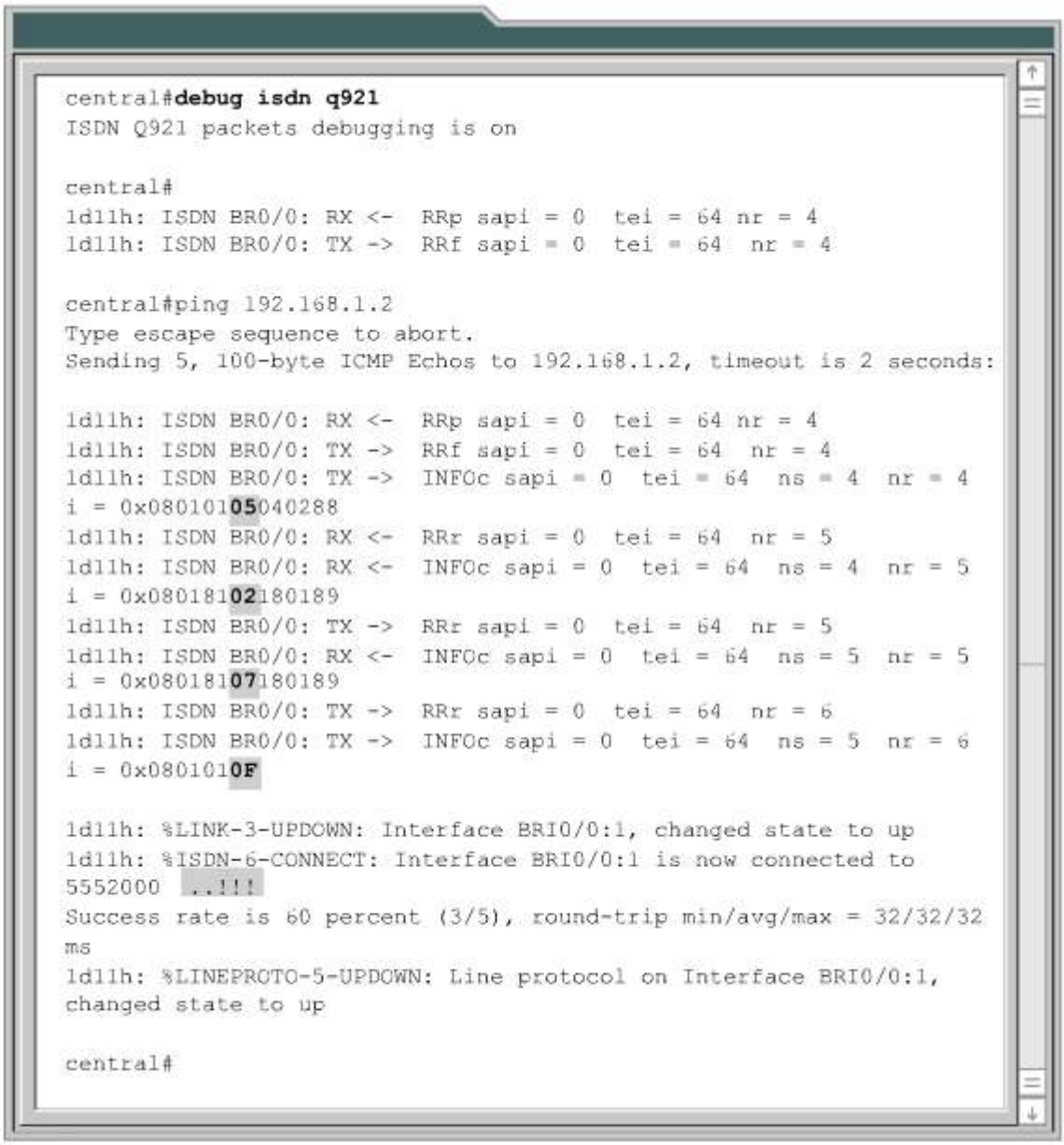
```
Phoenix#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
ACTIVE
    Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
TEI = 65, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
TEI 64, ces = 1, state = 8(established)
    spid1 configured, no LDN, spid1 sent, spid1 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 1
TEI 65, ces = 2, state = 8(established)
    spid2 configured, no LDN, spid2 sent, spid2 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 2
    Layer 3 Status:
1 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 1
CCB:callid=8001, sapi=0, ces=1, B-chan=1, calltype=DATA
```

Dans cet écran, la couche 1 RNIS est active, la couche 2 RNIS est établie avec SPID1 et SPID2 validés, et il y a une connexion active sur la couche 3.

4.3.9 Dépannage de la configuration DDR

Il existe deux grandes catégories de problèmes DDR. Soit un routeur ne numérote pas quand il le devrait, soit il numérote constamment quand il ne le devrait pas. Plusieurs commandes **debug** peuvent être utilisées pour faciliter le dépannage d'une configuration DDR.

Dans les lignes suivantes, les septième et huitième nombres hexadécimaux les plus significatifs indiquent le type de message. 1



```
central#debug isdn q921
ISDN Q921 packets debugging is on

central#
1d11h: ISDN BR0/0: RX <-  RRp sapi = 0  tei = 64 nr = 4
1d11h: ISDN BR0/0: TX ->  RRf sapi = 0  tei = 64  nr = 4

central#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:

1d11h: ISDN BR0/0: RX <-  RRp sapi = 0  tei = 64 nr = 4
1d11h: ISDN BR0/0: TX ->  RRf sapi = 0  tei = 64  nr = 4
1d11h: ISDN BR0/0: TX ->  INFOc sapi = 0  tei = 64  ns = 4  nr = 4
i = 0x08010105040288
1d11h: ISDN BR0/0: RX <-  RRr sapi = 0  tei = 64  nr = 5
1d11h: ISDN BR0/0: RX <-  INFOc sapi = 0  tei = 64  ns = 4  nr = 5
i = 0x08018102180189
1d11h: ISDN BR0/0: TX ->  RRr sapi = 0  tei = 64  nr = 5
1d11h: ISDN BR0/0: RX <-  INFOc sapi = 0  tei = 64  ns = 5  nr = 5
i = 0x08018107180189
1d11h: ISDN BR0/0: TX ->  RRr sapi = 0  tei = 64  nr = 6
1d11h: ISDN BR0/0: TX ->  INFOc sapi = 0  tei = 64  ns = 5  nr = 6
i = 0x0801010F

1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
1d11h: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000  ..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 32/32/32
ms
1d11h: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1,
changed state to up

central#
```

- 0x05 indique un message d'établissement d'appel
- 0x02 indique un message de traitement d'appel
- 0x07 indique un message de connexion d'appel
- 0x0F indique un message d'accusé de réception (ack) correct

La commande **debug isdn q931** s'avère utile pour observer les échanges lors de l'établissement d'appels sortants et entrants. 2 – 3

```
central#debug isdn q931
ISDN Q931 packets debugging is on
central#ping 192.168.1.2

1d11h: ISDN BR0/0: TX ->  SETUP pd = 8  callref = 0x02
1d11h:         Bearer Capability i = 0x8890
1d11h:         Channel ID i = 0x83
1d11h:         Keypad Facility i = '5552000'
1d11h: ISDN BR0/0: RX <-  CALL_PROC pd = 8  callref = 0x82
1d11h:         Channel ID i = 0x89
1d11h: ISDN BR0/0: RX <-  CONNECT pd = 8  callref = 0x82
1d11h:         Channel ID i = 0x89
1d11h: ISDN BR0/0: TX ->  CONNECT_ACK pd = 8  callref = 0x02
1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
1d11h: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000 .!!!!
```

```
remote#debug isdn q931
1d11h: ISDN BR0/0: RX <-  SETUP pd = 8  callref = 0x02
1d11h:         Bearer Capability i = 0x8890
1d11h:         Channel ID i = 0x89
1d11h:         Signal i = 0x40 - Alerting on - pattern 0
1d11h:         Called Party Number i = 0xC1, '5552000'
1d11h: ISDN BR0/0: Event: Received a DATA call from <unknown> on B1
at 64 Kb/s
1d11h: ISDN BR0/0: TX ->  CALL_PROC pd = 8  callref = 0x82
1d11h:         Channel ID i = 0x89
1d11h: ISDN BR0/0: TX ->  CONNECT pd = 8  callref = 0x82
1d11h:         Channel ID i = 0x89
1d11h: ISDN BR0/0: RX <-  CONNECT_ACK pd = 8  callref = 0x02
1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
```

La commande **debug dialer [events | packets]** permet de résoudre les problèmes de connectivité DDR. La commande **debug dialer events** envoie à la console un message lui indiquant quand une liaison DDR s'est établie et le trafic à l'origine de la connexion. 4

```
central#debug dialer events
Dial on demand events debugging is on

central#ping 192.168.1.2
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
192.168.1.2, timeout is 2 seconds:

1d11h: BR0/0 DDR: rotor dialout [priority]
1d11h: BR0/0 DDR: Dialing cause ip (s=192.168.1.1, d=192.168.1.2)
1d11h: BR0/0 DDR: Attempting to dial 5554000
1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
1d11h: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000 ..!!!
```

Le résultat de la commande debug dialer events indique le trafic intéressant à l'origine de la connexion du circuit DDR.

Si un routeur n'est pas configuré correctement pour DDR, les résultats renvoyés par la commande indiquent généralement la source du problème. Si aucun résultat de débogage ne s'affiche, le routeur ne reconnaît aucun trafic intéressant. La configuration incorrecte d'un numéroteur ou d'une liste d'accès peut en être la cause.

Tous les problèmes DDR ne se traduisent pas par l'impossibilité de numéroter pour une interface. Les protocoles de routage peuvent mener une interface à numéroter constamment, même s'il n'y a pas de données utilisateur à envoyer. On dit d'une interface qui s'active et se désactive en permanence qu'elle est en battement. La commande **`debug dialer packet`** envoie un message à la console à chaque fois qu'un paquet est envoyé d'une interface DDR. Utilisez-la pour déterminer exactement le trafic responsable du battement d'une interface DDR

Si un routeur ne se connecte pas quand il le devrait, il est alors possible que le problème soit lié à l'accès RNIS et non à l'interface DDR. Il se peut que le routeur distant soit mal configuré ou qu'un problème soit survenu sur le réseau de l'opérateur RNIS. La commande **`isdn call interface`** force le routeur local à accéder au routeur distant. 5

```
central#isdn call interface bri0/0 5552000

1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
1d11h: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000
```

La commande isdn call interface force un routeur à se connecter, quelle que soit sa configuration DDR.

Si les routeurs ne peuvent pas communiquer avec cette commande, la perte de connectivité est un problème RNIS et non DDR. En revanche, si les routeurs peuvent communiquer, cela signifie que le réseau interurbain et les configurations RNIS des routeurs fonctionnent correctement. Dans ce cas, il s'agit probablement d'une erreur de configuration DDR sur l'un des routeurs.

Dans certains cas, il est préférable de réinitialiser la connexion entre le routeur et le commutateur RNIS local. La commande **`clear interface bri`** annule les connexions actives sur l'interface et réinitialise celle-ci avec le commutateur RNIS. Cette commande force le routeur à renégocier ses SPID avec le commutateur RNIS et s'avère parfois nécessaire après avoir apporté des modifications aux commandes **`isdn spid1`** et **`isdn spid2`** sur une interface.

Activité de TP

Activité en ligne: isdn spid

Au cours de cette activité, l'étudiant va apprendre comment utiliser la commande **`isdn spid`** pour définir, au niveau du routeur, le numéro de l'identificateur de profil de service qui a été attribué par le service RNIS fourni sur le canal B1.

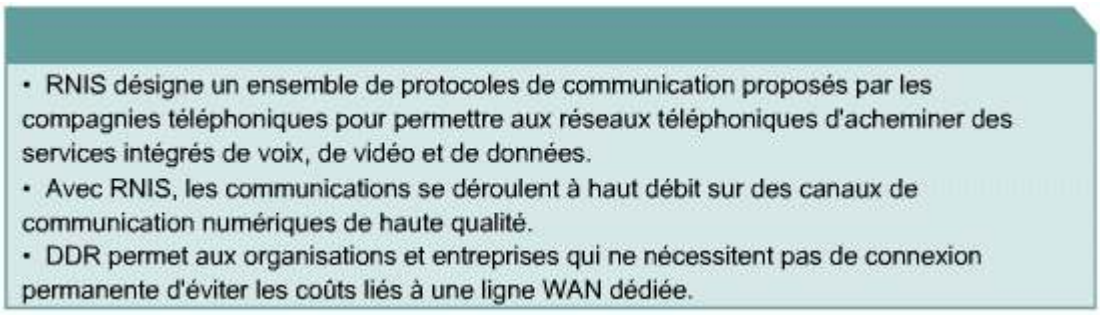
Résumé

RNIS désigne un ensemble de protocoles de communication proposés par les compagnies téléphoniques pour permettre aux réseaux téléphoniques d'acheminer des services intégrés de voix, vidéo et données. Avec RNIS, les communications se déroulent à haut débit sur des canaux de communication numériques de haute qualité.

DDR permet aux organisations et entreprises qui ne nécessitent pas de connexion permanente d'éviter les coûts liés à une ligne WAN dédiée. Il peut également être utilisé en tant que ligne de secours par les entreprises qui utilisent la ligne dédiée pour des applications critiques.

La compréhension des points clés suivants devrait être acquise:

- La technologie RNIS achemine des données, de la voix et de la vidéo
- La technologie RNIS utilise des normes pour l'adressage, les concepts et la signalisation
- La technologie RNIS utilise les couches physique et de liaison de données
- Les interfaces et les points de référence pour RNIS
- La configuration du routeur pour RNIS
- Quel trafic est autorisé en configurant DDR
- Les routes statiques pour DDR
- Le type d'encapsulation approprié à DDR
- Les listes d'accès agissant sur le trafic DDR
- Les interfaces de numérotation


• RNIS désigne un ensemble de protocoles de communication proposés par les compagnies téléphoniques pour permettre aux réseaux téléphoniques d'acheminer des services intégrés de voix, de vidéo et de données.
• Avec RNIS, les communications se déroulent à haut débit sur des canaux de communication numériques de haute qualité.
• DDR permet aux organisations et entreprises qui ne nécessitent pas de connexion permanente d'éviter les coûts liés à une ligne WAN dédiée.

Vue d'ensemble

La technologie Frame Relay a été développée à l'origine en tant qu'extension du RNIS. Elle a été conçue pour permettre l'acheminement de la technologie à commutation de circuits sur un réseau à commutation de paquets. Cette technologie est devenue un moyen autonome et économique de créer un réseau WAN.

Les commutateurs Frame Relay créent des circuits virtuels permettant de connecter des réseaux locaux distants à un WAN. Le réseau Frame Relay existe entre un équipement frontière de réseau local, généralement un routeur, et le commutateur de l'opérateur. La technologie utilisée par l'opérateur pour acheminer les données entre les commutateurs n'a pas d'importance pour Frame Relay.

La complexité de la technologie exige une connaissance approfondie des termes décrivant le fonctionnement de Frame Relay. En effet, sans une compréhension totale du réseau Frame Relay, il s'avère difficile d'y effectuer des dépannages.

Frame Relay est devenu l'un des protocoles WAN les plus répandus. L'une des raisons de sa popularité est notamment son faible coût par rapport à celui de lignes louées. Frame Relay est également populaire parce que les procédures de configuration de l'équipement utilisateur d'un réseau Frame Relay sont très simples.

Ce module explique comment configurer Frame Relay sur un routeur Cisco. Pour créer des connexions Frame Relay, il faut configurer des routeurs ou d'autres équipements pour les faire communiquer avec un commutateur Frame Relay. C'est généralement le fournisseur d'accès qui configure ce commutateur. Cela aide à maintenir les tâches de configuration utilisateur à un niveau minimum.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

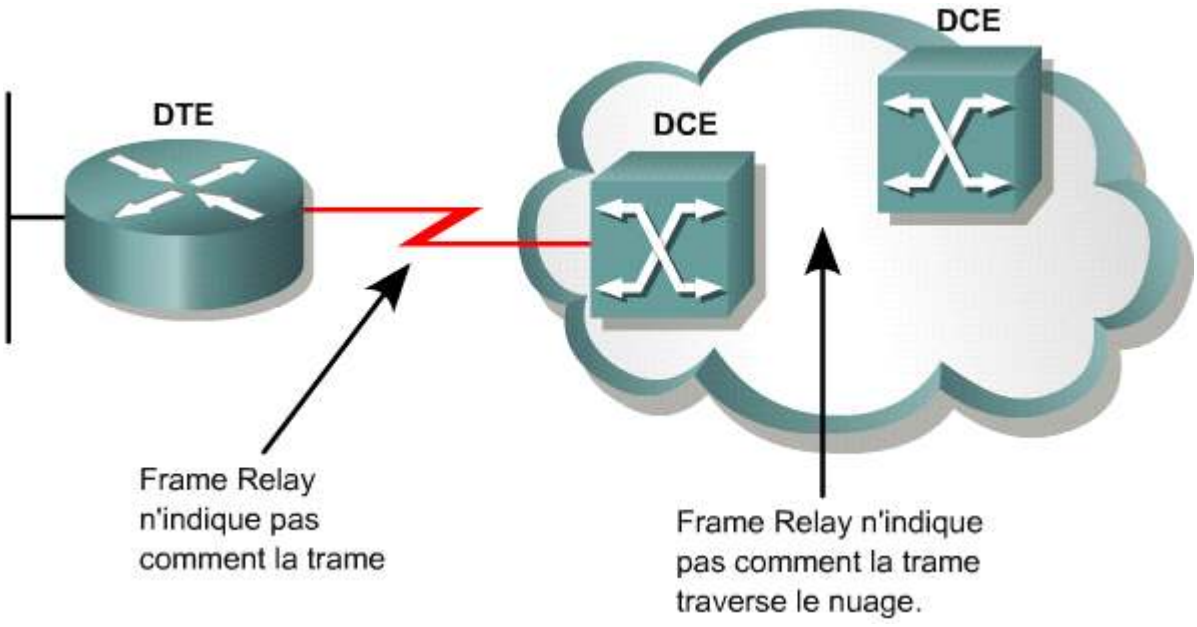
- Expliquer la portée et la fonction de Frame Relay
- Discuter la technologie de Frame Relay
- Comparer les topologies point-à-point et point-à-multipoint
- Examiner la topologie d'un réseau Frame Relay
- Configurer un circuit virtuel permanent (PVC – *Permanent Virtual Circuit*) Frame Relay
- Créer une carte Frame Relay sur un réseau distant
- Expliquer les problèmes liés à un réseau à accès multiple non-broadcast
- Décrire le besoin de sous-interfaces et leur mode de configuration
- Vérifier et dépanner une connexion Frame Relay

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
5.1	Concepts Frame Relay
5.2	Configuration de Frame Relay

5.1 Concepts Frame Relay

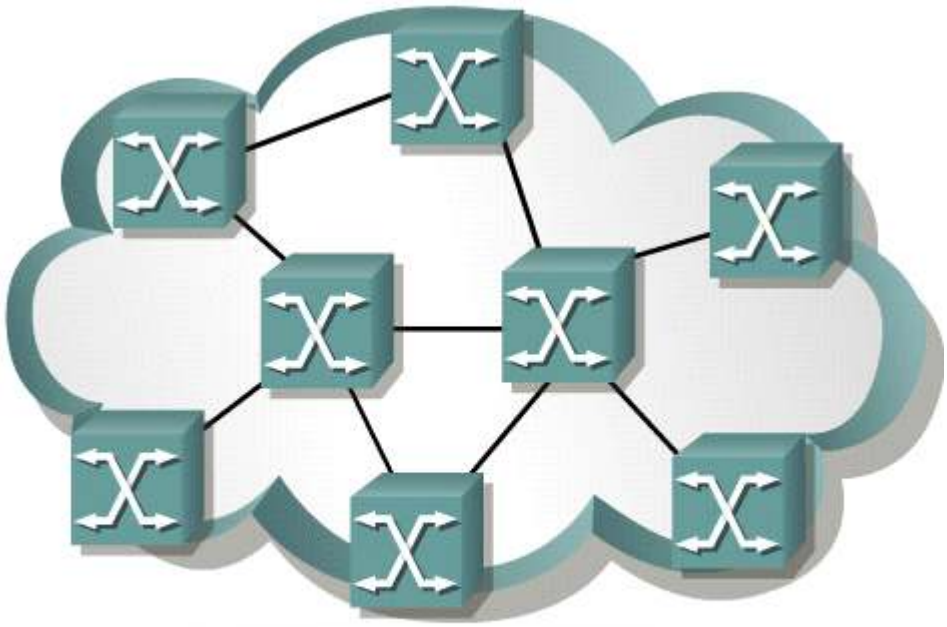
5.1.1 Présentation de Frame Relay

Frame Relay est une norme de l'UIT-T (*Union internationale des télécommunications – secteur de normalisation des télécommunications*) et de l'ANSI (*American National Standards Institute*). Frame Relay est un service WAN à commutation de paquets orienté connexion. Il fonctionne au niveau de la couche liaison de données du modèle OSI. Frame Relay utilise un sous-ensemble du protocole HDLC (*high-level data-link control*) dénommé LAPF (*Link Access Procedure for Frame Relay*). Des trames acheminent les données entre des équipements utilisateur nommés équipements terminaux de traitement de données (ETTD) et l'équipement de communication de données (ETCD) situé à la périphérie du WAN. [1]

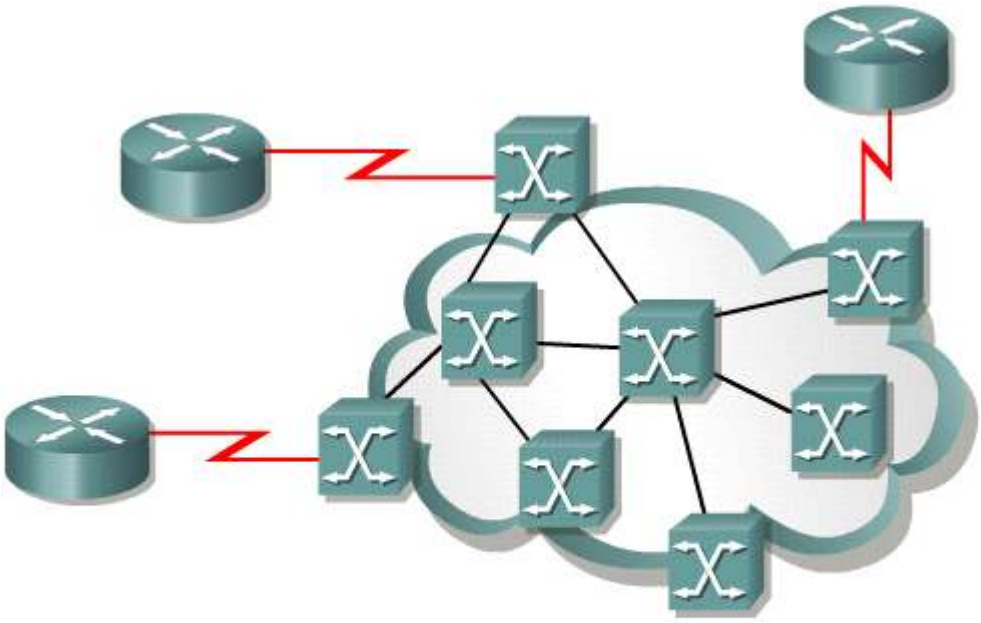


À l'origine, Frame Relay a été conçu pour permettre à l'équipement RNIS de disposer d'un accès vers un service à commutation de paquets sur un canal B. Toutefois, Frame Relay est aujourd'hui une technologie autonome.

Un réseau Frame Relay peut appartenir à un particulier, mais il est la plupart du temps proposé comme service par un opérateur public. Il consiste généralement en de nombreux commutateurs Frame Relay dispersés géographiquement et interconnectés par des lignes agrégées. [2] [3]

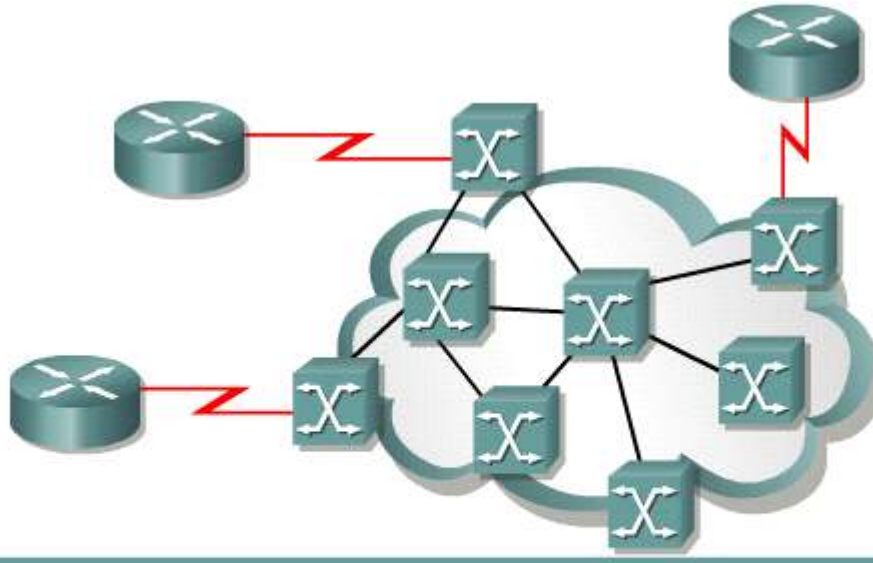


Le réseau WAN Frame Relay est une toile de commutateurs interconnectés.

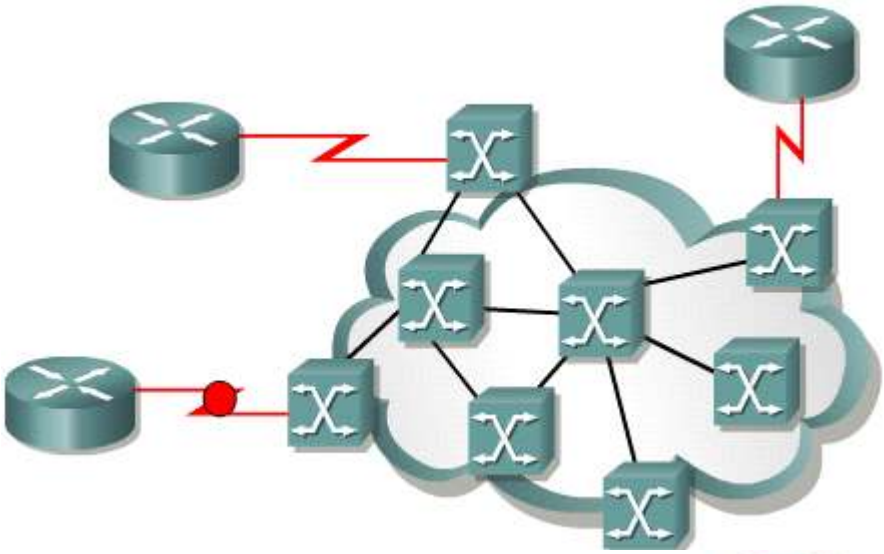


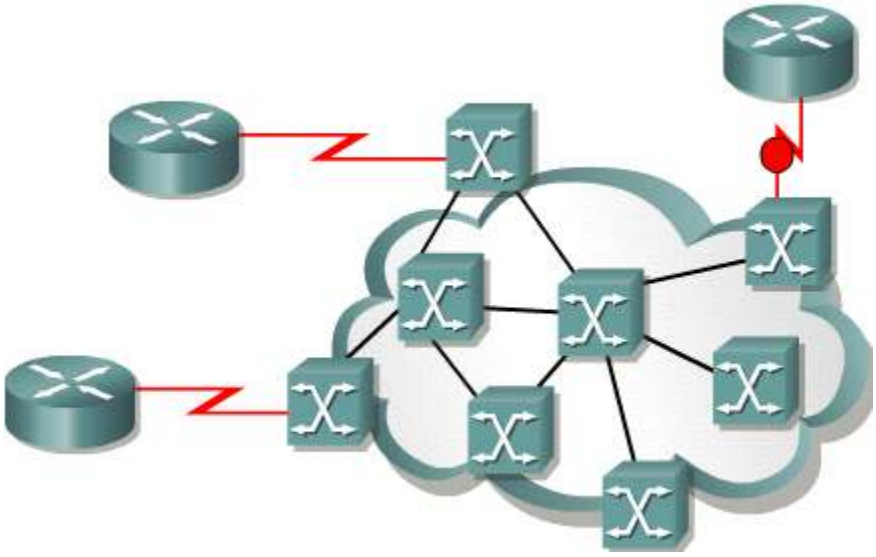
Le réseau WAN Frame Relay est une toile de commutateurs interconnectés. Les ETTD des clients se connectent aux commutateurs par le biais de lignes louées.

Frame Relay sert souvent à interconnecter des réseaux locaux. Quand c'est le cas, un routeur sur chaque réseau local sert d'ETTD. Une connexion série, telle qu'une ligne louée T1/E1, connecte le routeur à un commutateur Frame Relay au niveau du point de présence le plus proche de l'opérateur. Le commutateur Frame Relay est un équipement ETCD. Les trames d'un ETTD sont déplacées sur le réseau et remises à d'autres ETTD par l'intermédiaire d'unités ETCD. [4]



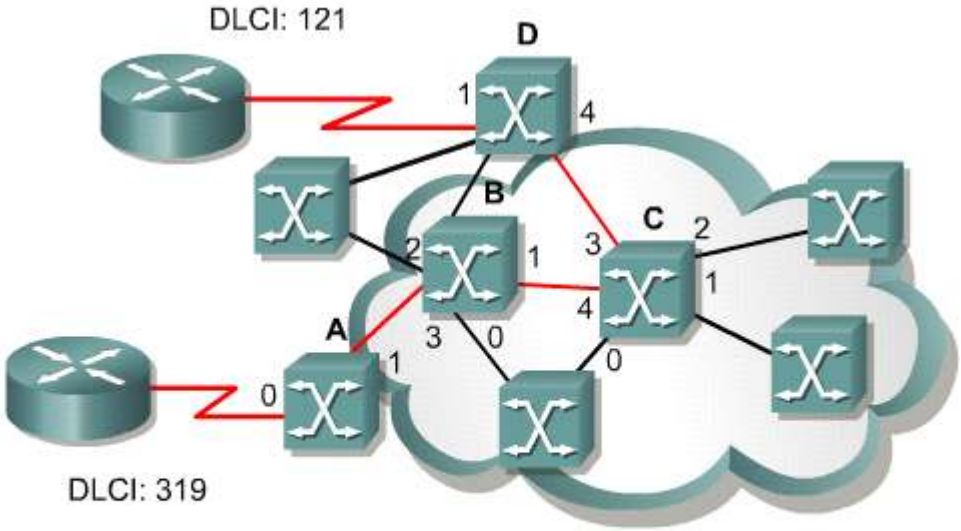
- L'équipement terminal de traitement de données (ETTD) envoie des trames à l'équipement de terminaison de circuit de données (ETCD).
- Les trames passent de commutateur en commutateur jusqu'à l'ETCD distant.
- L'ETCD distant les distribue à l'ETTD cible.





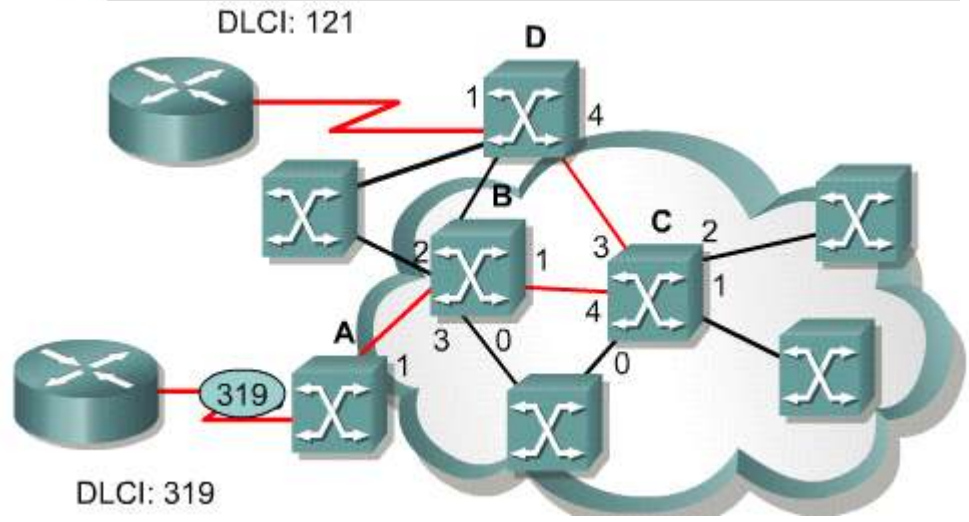
L'équipement informatique qui n'est pas sur un réseau local peut également envoyer des données sur un réseau Frame Relay. Cet équipement utilise une unité d'accès Frame Relay (FRAD – *Frame Relay access device*) en tant qu'ETTD.

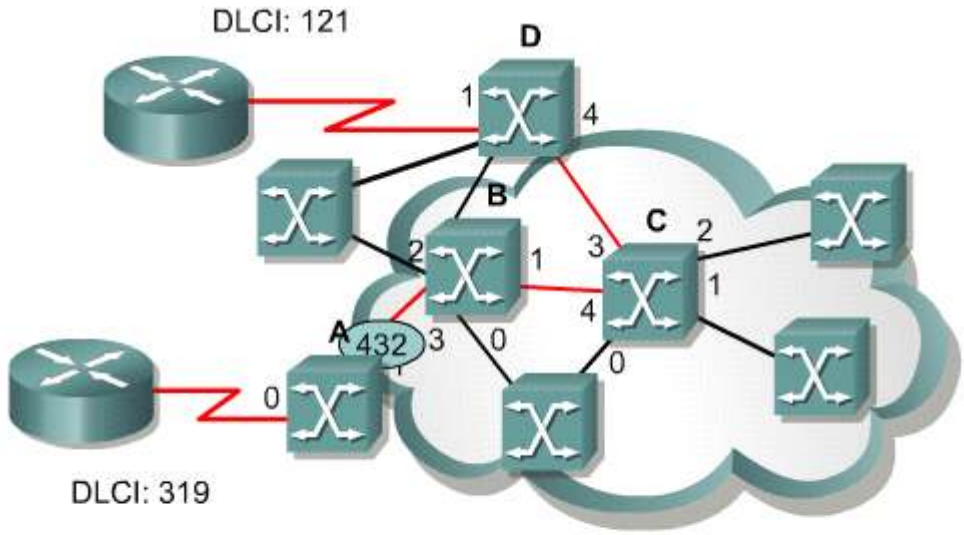
On appelle circuit virtuel (VC) la connexion entre deux ETTD par le réseau Frame Relay. Les circuits virtuels peuvent être établis de façon dynamique par l'envoi de messages de signalisation au réseau. Dans ce cas, on les appelle des circuits virtuels commutés (SVC *switched virtual circuits*). Toutefois, ces SVC ne sont pas très courants. En général, des circuits virtuels permanents (PVC) préconfigurés par l'opérateur sont utilisés. Un circuit virtuel est créé par le stockage d'un mappage entre port d'entrée et port de sortie dans la mémoire de chaque commutateur, afin de les lier jusqu'à ce qu'un chemin continu d'une extrémité à l'autre du circuit ait été identifié. [1]



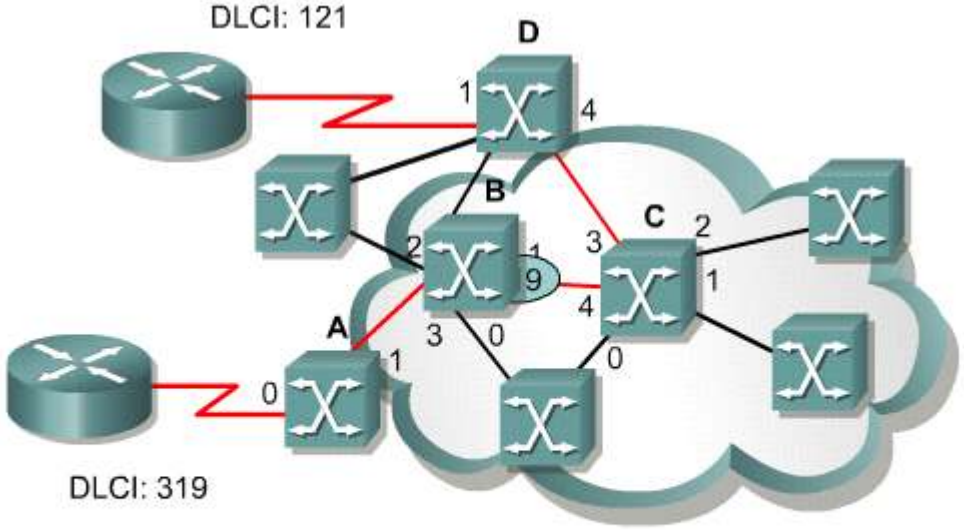
Fenêtre contextuelle

Les tables de chaque commutateur définissent un chemin ou un circuit virtuel entre deux ETTD.

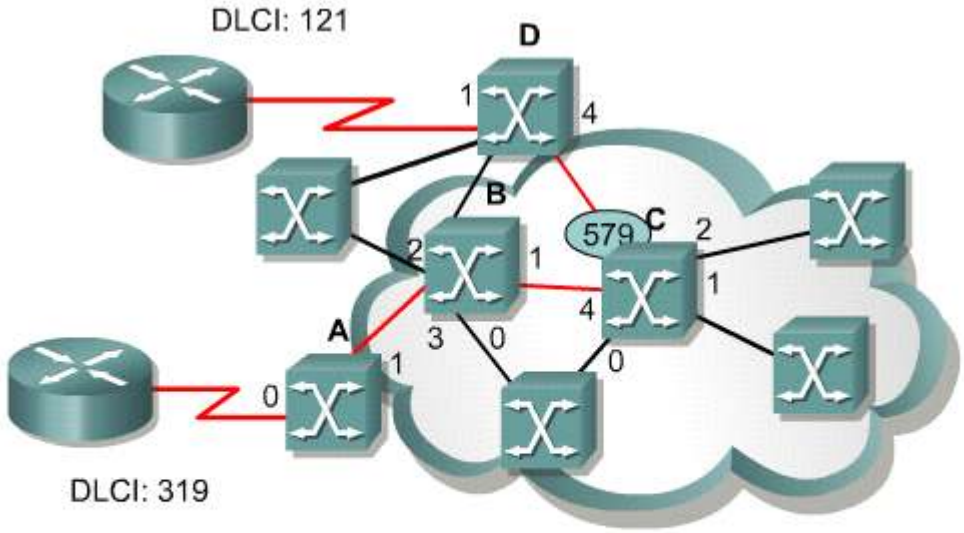




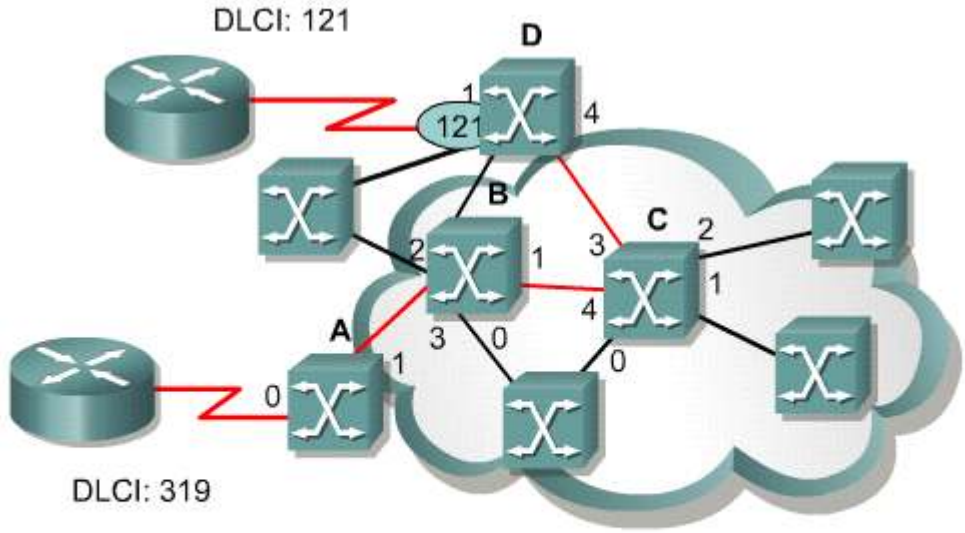
A			
VC	Port	VC	Port
319	0	432	1



B			
VC	Port	VC	Port
432	3	119	1



C			
VC	Port	VC	Port
119	4	579	3

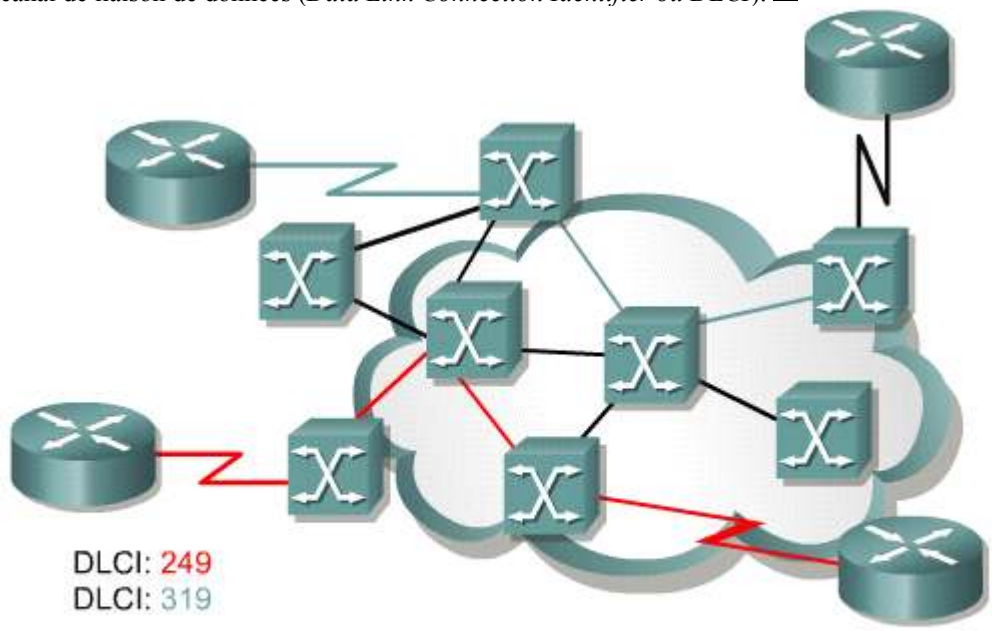


D			
VC	Port	VC	Port
579	0	121	1

Comme Frame Relay a été conçu pour fonctionner sur des lignes numériques de haute qualité, aucun mécanisme de récupération après erreur n'est fourni. Si un nœud détecte une erreur dans une trame, il la rejette sans notification.

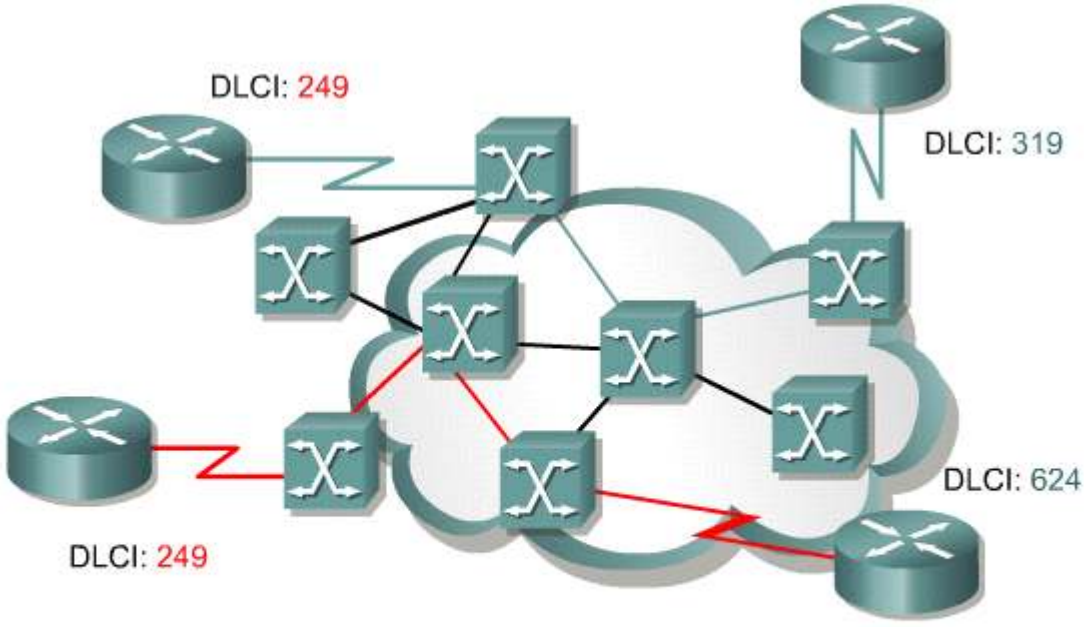
Le FRAD ou le routeur connecté au réseau peut être connecté à divers points d'extrémité par plusieurs circuits virtuels. Ceci remplace de façon très économique un maillage de lignes d'accès. Avec cette configuration, chaque point d'extrémité ne nécessite qu'une ligne d'accès et une interface. D'autres économies peuvent être réalisées, car la capacité de la ligne d'accès est fondée sur la bande passante moyenne requise par les circuits virtuels et non sur la bande passante maximale requise.

Les divers circuits virtuels d'une seule ligne d'accès peuvent être distingués, chaque VC disposant de son propre identificateur de canal de liaison de données (*Data Link Connection Identifier ou DLCI*). 2



L'identificateur DLCI permet de faire la distinction entre plusieurs circuits virtuels sur une même liaison d'accès.

L'identificateur DLCI est stocké dans le champ d'adresse de chaque trame transmise. Le DLCI n'a généralement qu'une signification locale et peut différer à chaque extrémité d'un circuit virtuel. 3



Les identificateurs DLCI ont une portée locale, ce qui signifie qu'ils sont spécifiques au canal physique sur lequel ils résident. En conséquence, les équipements situés à l'autre extrémité d'une connexion peuvent utiliser des identificateurs DLCI différents pour faire référence à la même connexion virtuelle.

Activité de média interactive

Glisser-Positionner: Terminologie Frame Relay

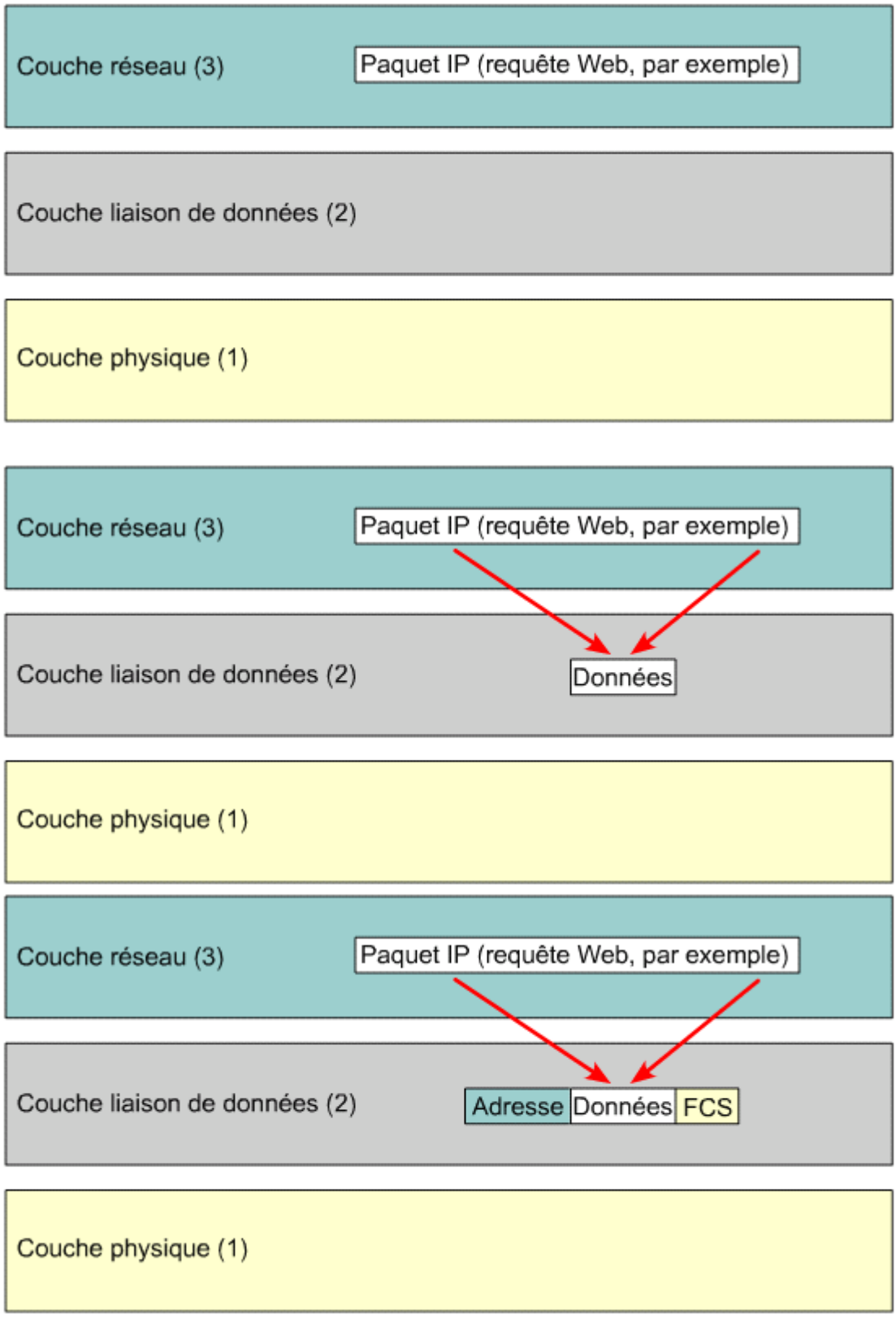
À la fin de cette activité, l'étudiant sera en mesure d'identifier correctement la terminologie liée à Frame Relay.

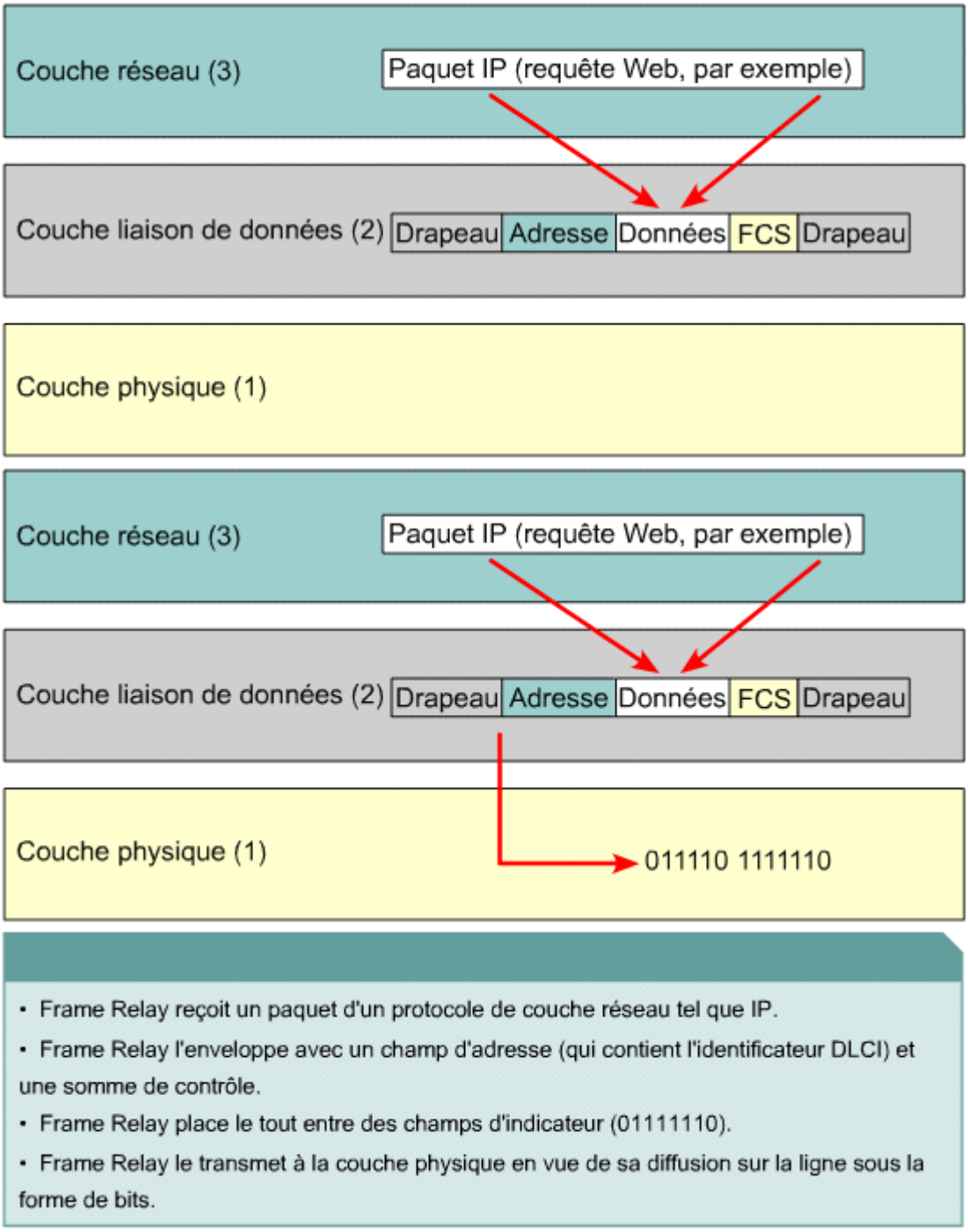
5.1 Concepts Frame Relay

5.1.3 Couches support de la pile Frame Relay

Frame Relay fonctionne comme suit:

- Prélèvement de paquets de données d'un protocole de couche réseau, tel qu'IP ou IPX
- Encapsulation de ces paquets comme partie données d'une trame Frame Relay [1] [2]




Couche réseau (3)
Paquet IP (requête Web, par exemple)
Couche liaison de données (2)
Drapeau
Adresse
Données
FCS
Drapeau
Couche physique (1)
Couche réseau (3)
Paquet IP (requête Web, par exemple)
Couche liaison de données (2)
Drapeau
Adresse
Données
FCS
Drapeau
Couche physique (1)
011110 1111110
• Frame Relay reçoit un paquet d'un protocole de couche réseau tel que IP.
• Frame Relay l'enveloppe avec un champ d'adresse (qui contient l'identificateur DLCI) et une somme de contrôle.
• Frame Relay place le tout entre des champs d'indicateur (01111110).
• Frame Relay le transmet à la couche physique en vue de sa diffusion sur la ligne sous la forme de bits.

- Transfert de ces trames vers la couche physique pour les délivrer sur la ligne

La séquence de contrôle de trame (FCS) sert à déterminer si des erreurs se sont produites dans le champ d'adresse de couche 2 au cours de la transmission. La FCS est calculée avant la transmission et le résultat est inséré dans le champ FCS. À l'extrémité distante, une deuxième valeur FCS est calculée et comparée à la FCS de la trame. Si les résultats sont identiques, la trame est traitée. S'ils diffèrent, la trame est abandonnée. Aucun avertissement n'est envoyé à la source quand une trame est abandonnée. Le contrôle d'erreur est laissé aux couches supérieures du modèle OSI.

5.1 Concepts Frame Relay

5.1.4 Bande passante et contrôle de flux Frame Relay

La connexion série ou le lien d'accès au réseau Frame Relay est généralement une ligne louée. La vitesse de la ligne est assujettie au débit d'accès ou du port. Les vitesses des ports s'échelonnent généralement entre 64 kbits/s et 4 Mbits/s. Certains fournisseurs proposent des débits atteignant 45 Mbits/s.

En général, plusieurs circuits virtuels permanents utilisent la liaison d'accès, chacun d'entre eux disposant d'une bande passante dédiée. C'est ce que l'on appelle le débit de données garanti (CIR). Le CIR est le débit auquel le fournisseur d'accès accepte de recevoir des bits sur le circuit virtuel.

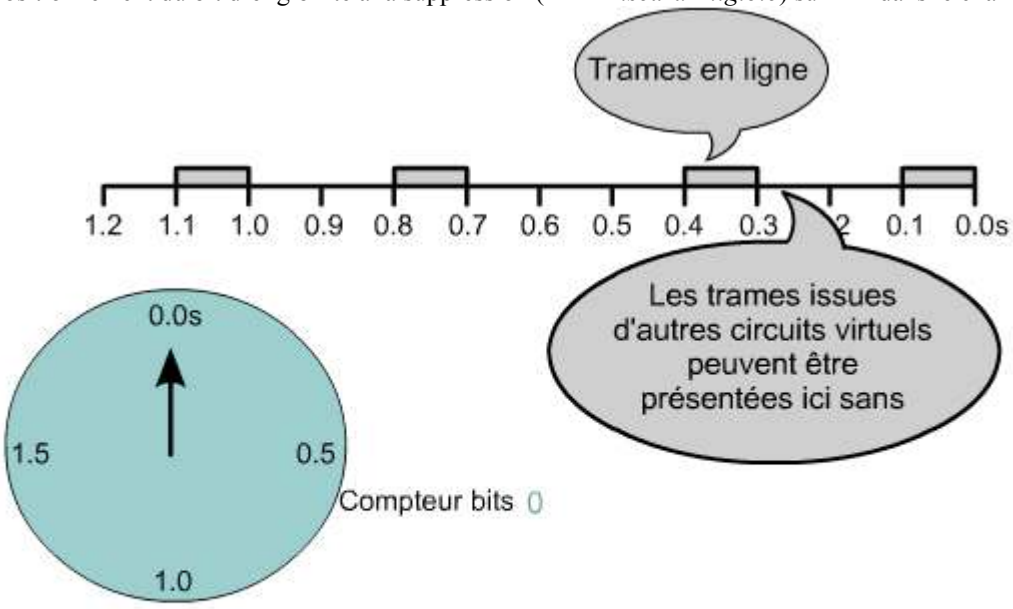
Les CIR individuels sont généralement inférieurs au débit du port. Toutefois, la somme des CIR est normalement supérieure au débit des ports. Le facteur peut parfois s'élever à 2 ou 3. Le multiplexage statistique s'adapte à la nature sporadique des communications informatiques, puisqu'il est peu probable que les canaux soient à leur débit maximal simultanément.

Pendant la transmission d'une trame, chaque bit est envoyé à la vitesse du port. C'est pourquoi il doit exister un écart entre les trames d'un circuit virtuel si le débit en bits moyen doit être le CIR.

Le commutateur accepte les trames de l'ETTD à des débits dépassant le CIR. Ceci fournit effectivement à chaque canal une bande passante à la demande jusqu'à un maximum défini par la vitesse du port. Certains fournisseurs d'accès imposent un débit maximum inférieur à la vitesse du port pour les circuits virtuels. La différence entre le CIR et le maximum, que celui-ci soit inférieur ou égal à la vitesse du port, est appelée EIR (*Excess Information Rate*).

L'intervalle de temps sur lequel les débits sont calculés est appelé la durée garantie (T_c). Le nombre de bits garantis dans T_c constitue le débit garanti en rafale (B_c). Le nombre de bits supplémentaires au-dessus du débit garanti en rafale, jusqu'à la vitesse maximale de la liaison d'accès est le débit garanti en excès (B_e).

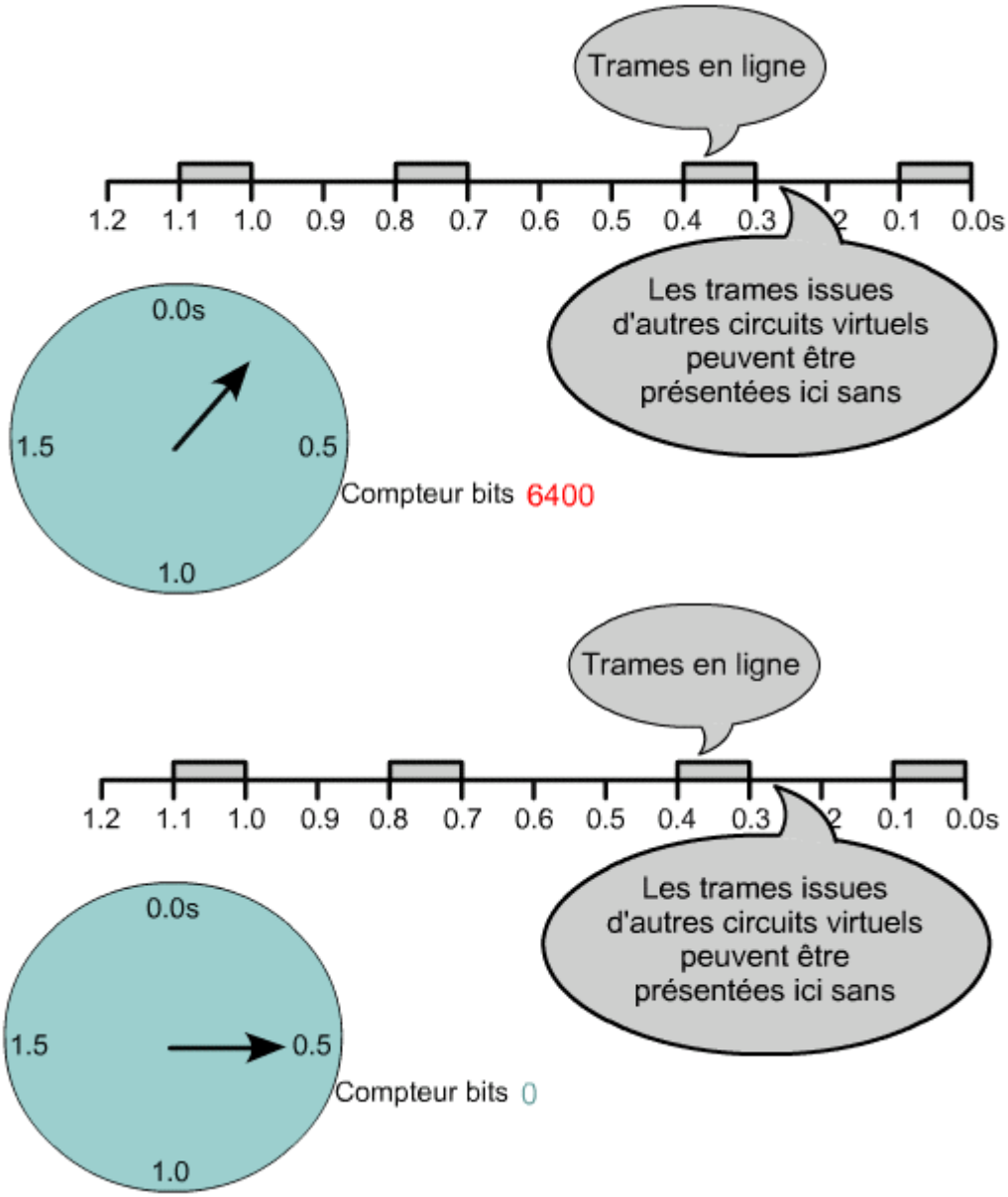
Bien que le commutateur accepte les trames excédant le CIR, chaque trame en excès est signalée au niveau du commutateur par le positionnement du bit d'éligibilité à la suppression (DE - *Discard Eligible*) sur «1» dans le champ d'adresse. 1 2 3

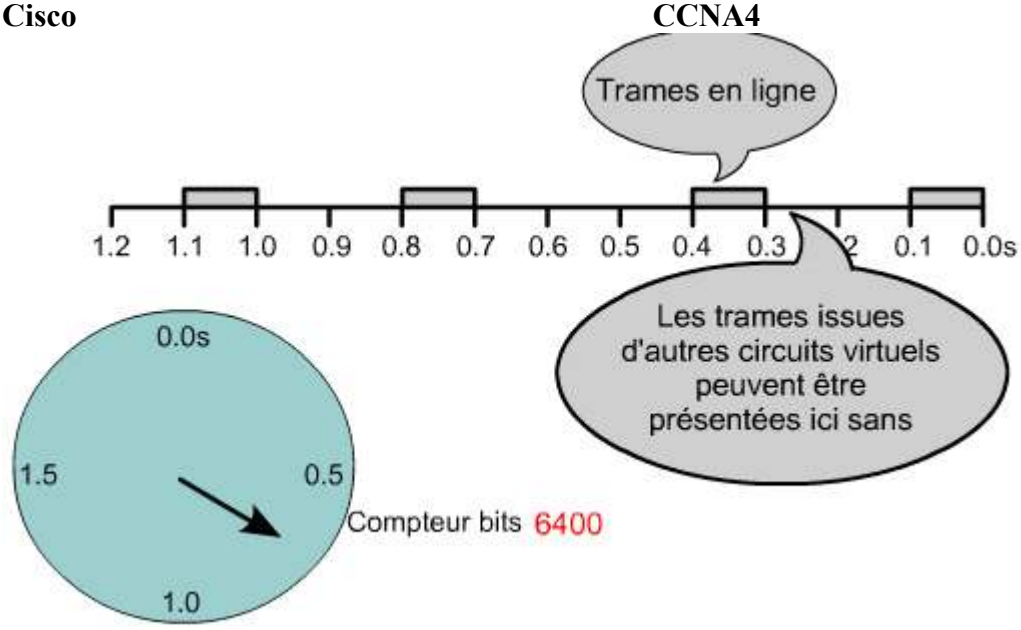


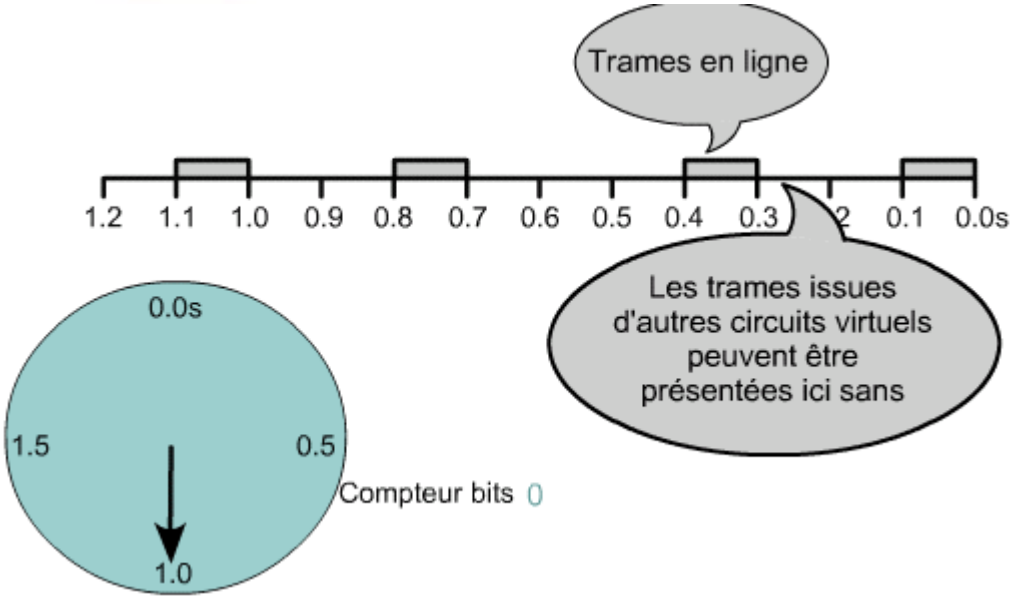
Une trame est présentée au début du premier intervalle. Elle est complète après 0,1 seconde. Aucune autre trame ne peut être présentée pendant 0,4 seconde sans pousser le compteur au-delà du niveau Bc (débit garanti en

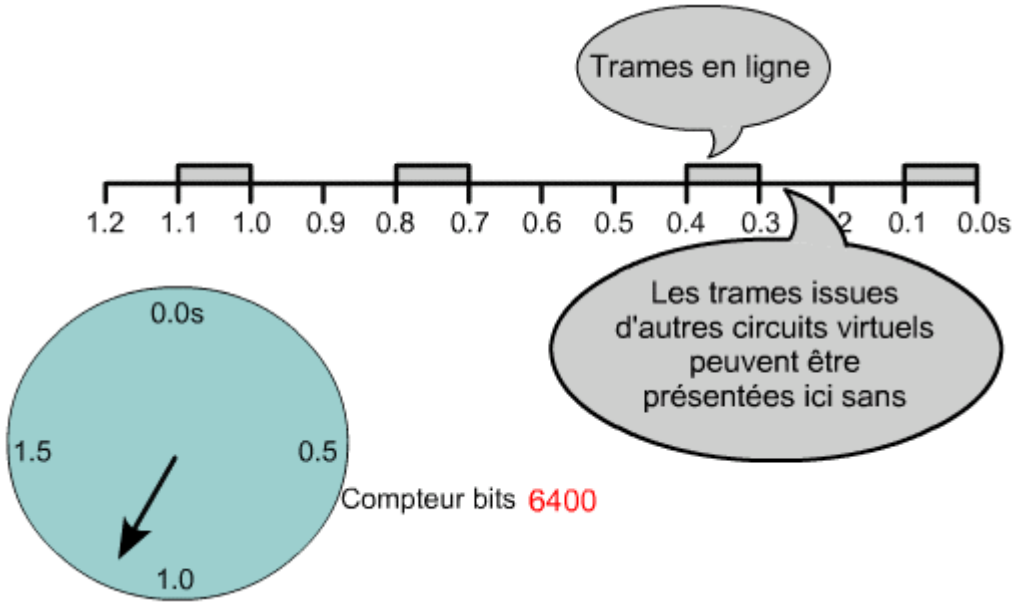
Fenêtre contextuelle

Valeurs fournies (Given values) :
Vitesse du port : 64 000 bits/s
Durée garantie (Tc) : 0,5 seconde
Débit de données garanti (CIR) : 12 800 bits/s
Valeur calculée (Calculated value) :
Débit garanti en rafale (Bc) (CIR x Tc) : 6 400 bits
À des fins de démonstration, prenez toutes les trames en 6 400 bits

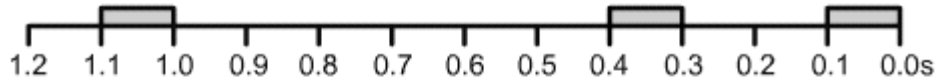

Trames en ligne
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0s
Les trames issues d'autres circuits virtuels peuvent être présentées ici sans
0.0s
1.5
0.5
1.0
Compteur bits 6400
Trames en ligne
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0s
Les trames issues d'autres circuits virtuels peuvent être présentées ici sans
0.0s
1.5
0.5
1.0
Compteur bits 0

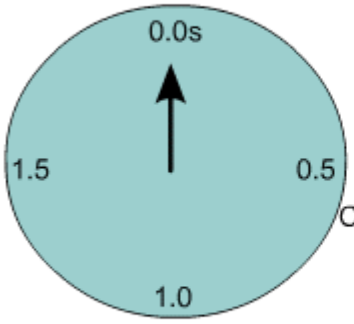

Trames en ligne
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 2 0.1 0.0s
Les trames issues d'autres circuits virtuels peuvent être présentées ici sans
0.0s
1.5
0.5
1.0
Compteur bits 6400


Trames en ligne
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 2 0.1 0.0s
Les trames issues d'autres circuits virtuels peuvent être présentées ici sans
0.0s
1.5
0.5
1.0
Compteur bits 0


Trames en ligne
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 2 0.1 0.0s
Les trames issues d'autres circuits virtuels peuvent être présentées ici sans
0.0s
1.5
0.5
1.0
Compteur bits 6400

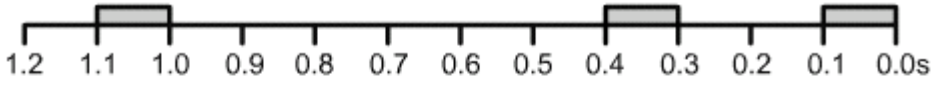
2-

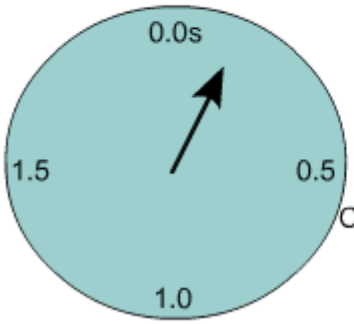




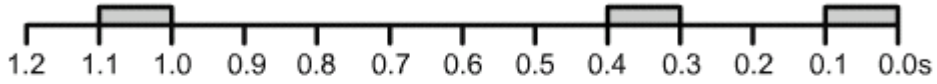
Compteur bits 0

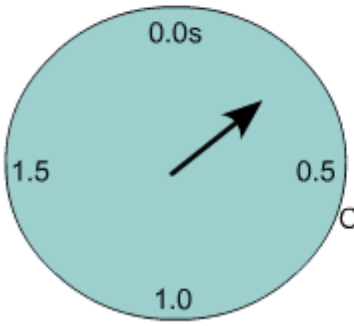
Si deux trames sont présentées dans le premier intervalle, la seconde est identifiée comme bit d'éligibilité à la suppression. Si une autre trame est présentée dans le second intervalle, elle est également identifiée de la sorte, jusqu'à ce que la moyenne revienne au niveau CIR.



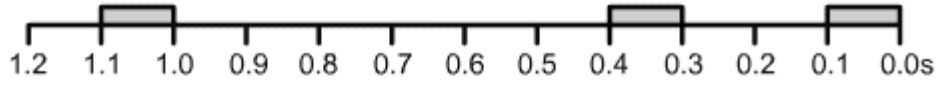


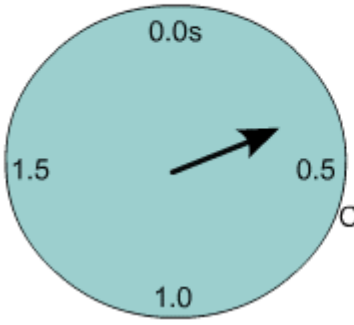
Compteur bits 6400



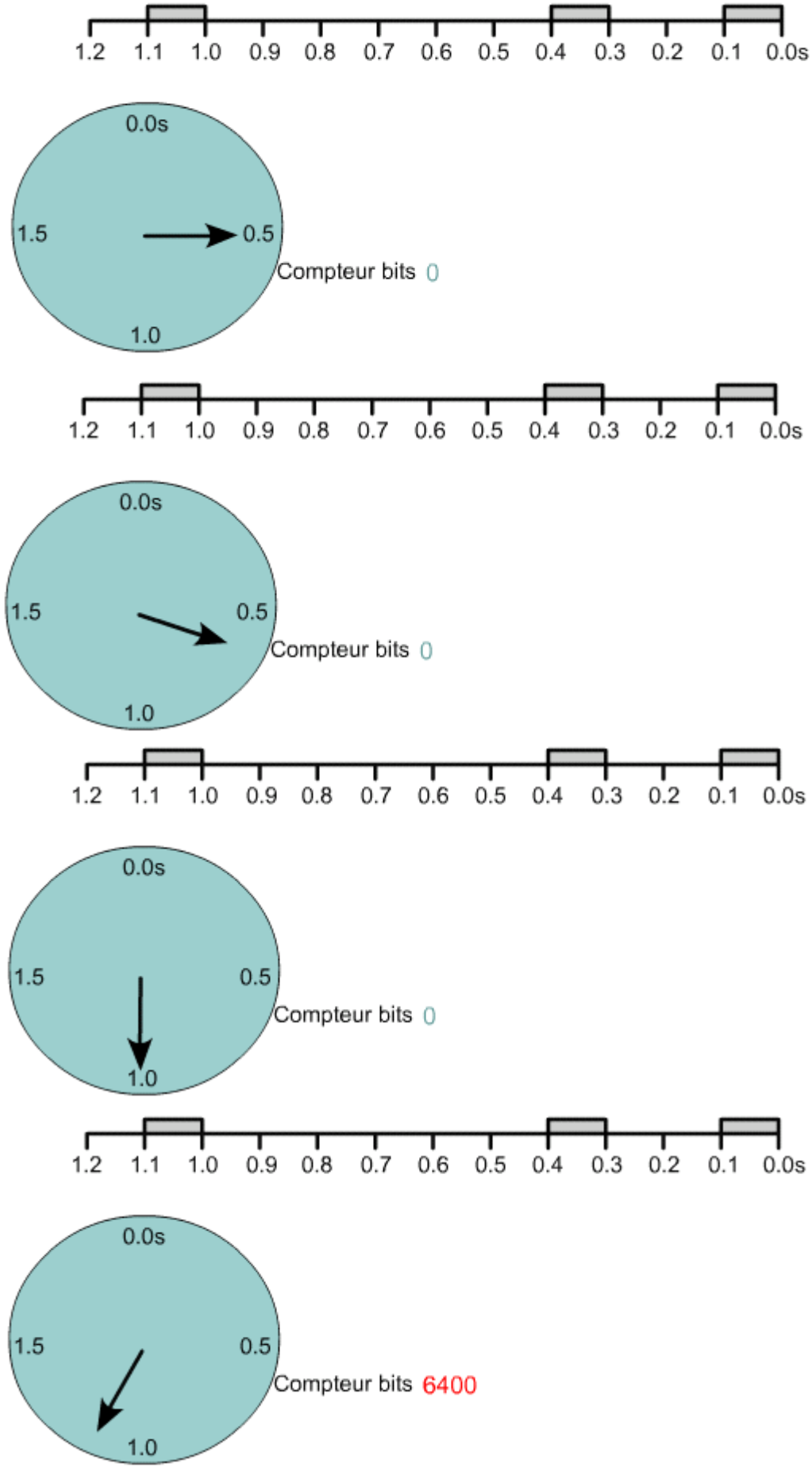


Compteur bits 12800

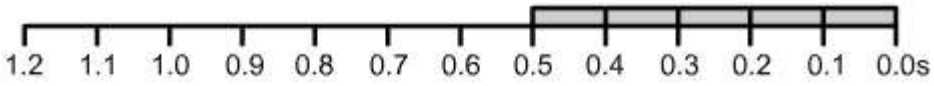


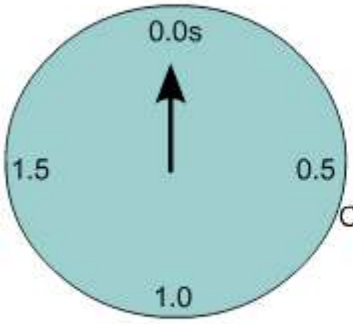


Compteur bits 6400


1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0s
0.0s
1.5
0.5
1.0
Compteur bits 0
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0s
0.0s
1.5
0.5
1.0
Compteur bits 0
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0s
0.0s
1.5
0.5
1.0
Compteur bits 0
1.2 1.1 1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0s
0.0s
1.5
0.5
1.0
Compteur bits 6400

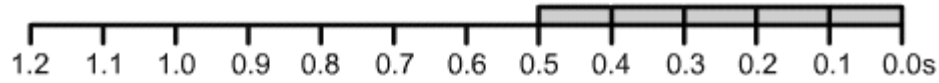
3-

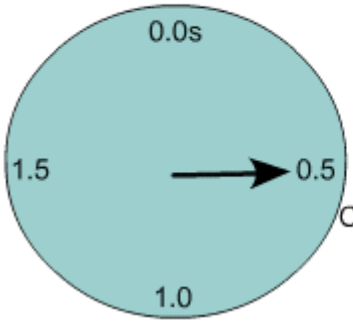




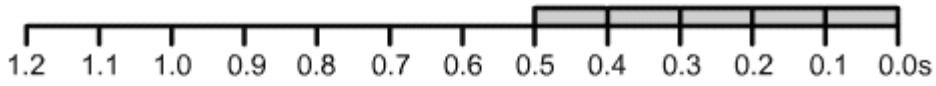
Compteur bits 0

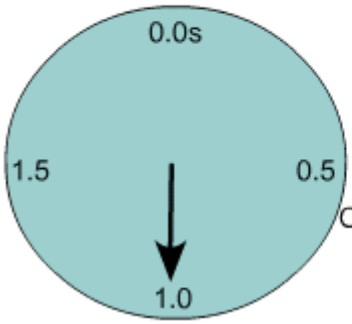
Si cinq trames (32 000 bits) sont présentées, toutes sont identifiées comme bits d'éligibilité à la suppression, à l'exception de la première. 2,5 secondes s'écouleront avant qu'une trame puisse être présentée et ne soit plus identifiée comme bit d'éligibilité à la suppression.



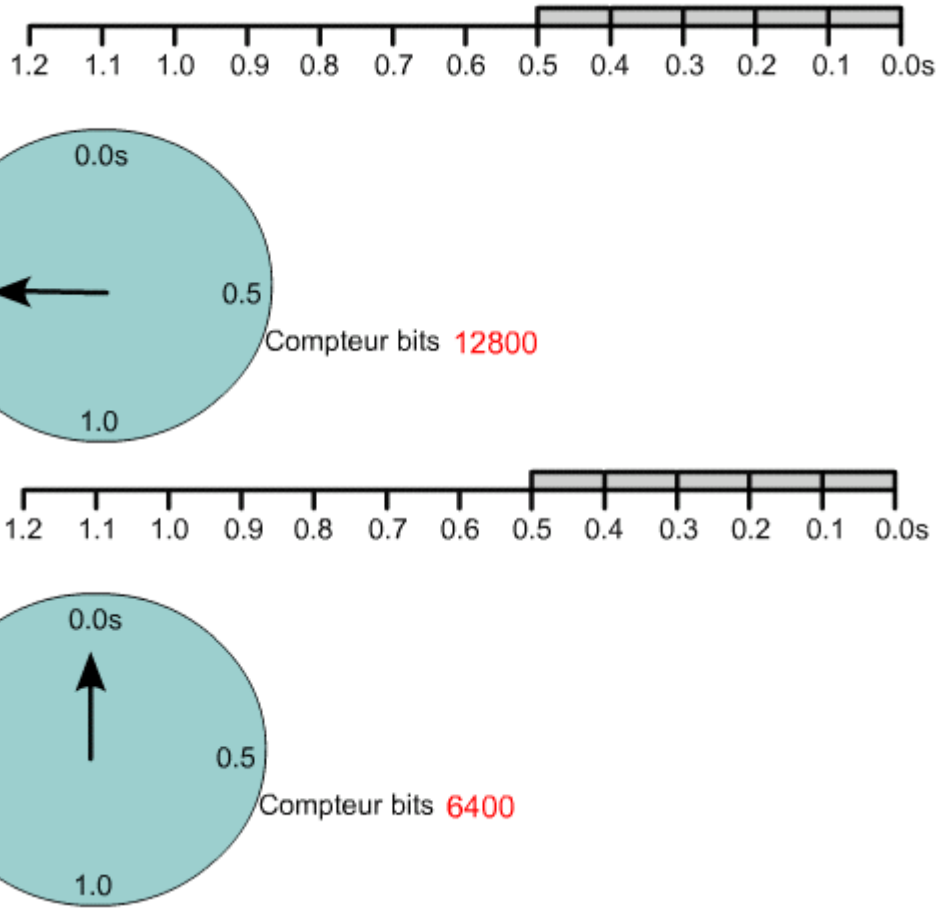


Compteur bits 25600





Compteur bits 19200



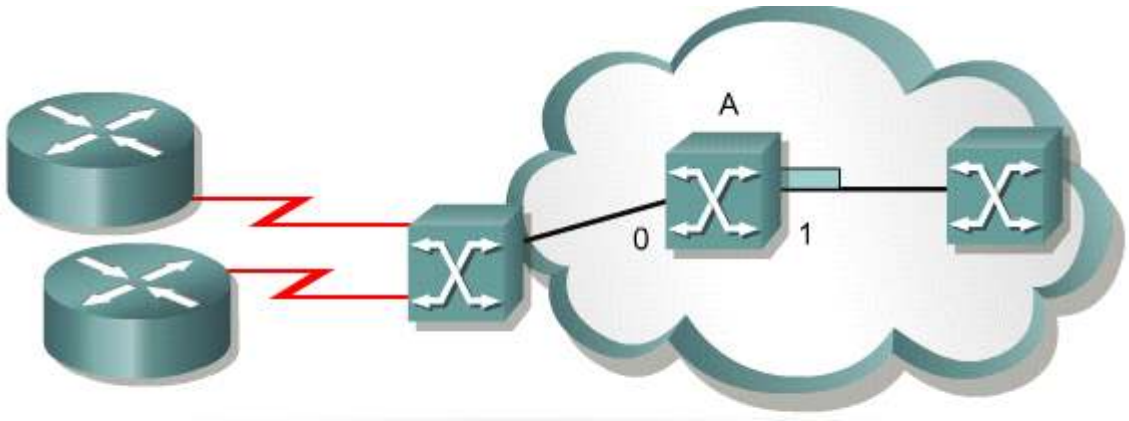
Le commutateur gère un compteur de bits pour chaque circuit virtuel. Une trame entrante est signalée comme DE si elle met le compteur au-delà de B_c. Une trame entrante est éliminée si elle pousse le compteur au-delà de $B_c + B_e$. À la fin de chaque T_c secondes, le compteur est réinitialisé. Comme le compteur ne peut pas être négatif, le temps d'inactivité ne peut pas être mis de côté.

Les trames qui arrivent au commutateur sont mises en file d'attente ou en tampon avant d'être transférées. Comme avec tous les systèmes de file d'attente, il se peut qu'une accumulation excessive de trames se produise au niveau du commutateur. Ceci occasionne des retards. Les retards mènent à des retransmissions inutiles, qui surviennent quand des protocoles de niveau supérieur ne reçoivent aucun accusé de réception au cours d'une période donnée. Dans les cas sévères, cela peut provoquer une chute sérieuse du débit du réseau.

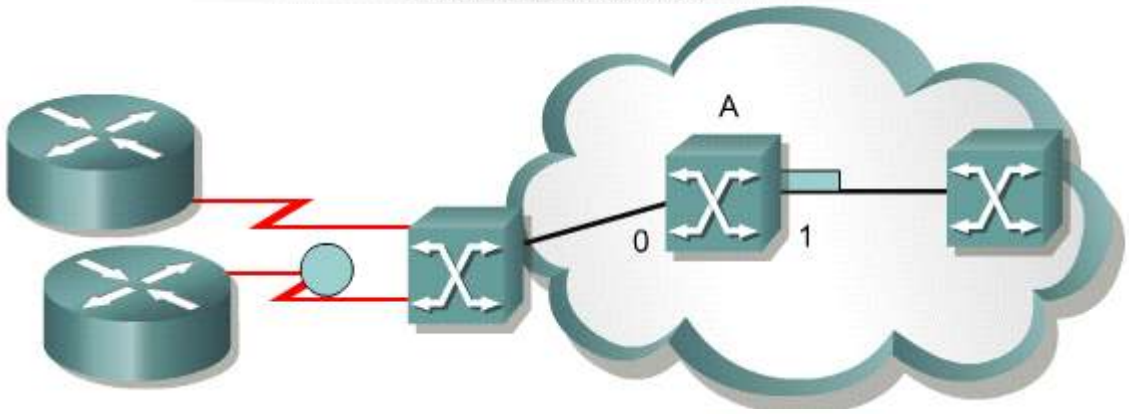
Pour éviter ce problème, les commutateurs Frame Relay appliquent une politique de rejet des trames en files d'attente pour que celles-ci restent courtes. Les trames dont le bit DE est défini sont supprimées en premier.

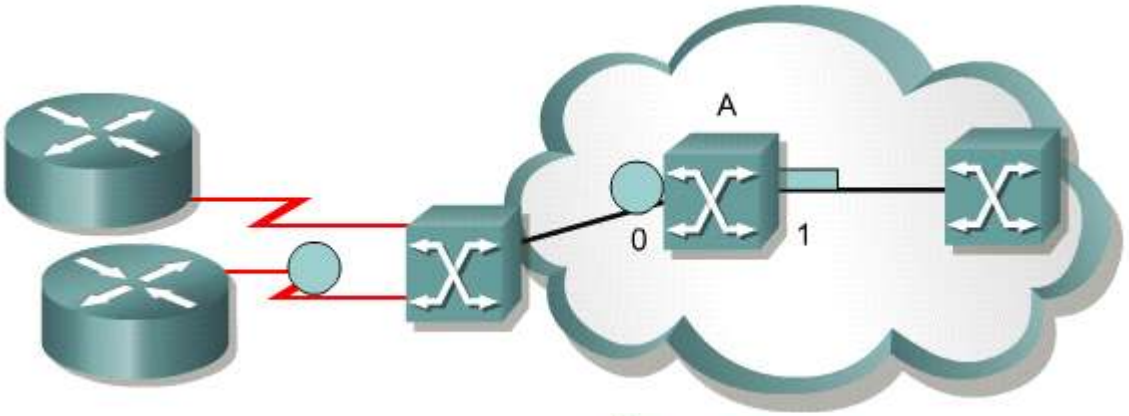
Quand un commutateur détermine que sa file d'attente augmente, il essaie de réduire le flux de trames y parvenant. Pour ce faire, il avertit les ETTD du problème en positionnant les bits de notification explicite de congestion (ECN – *Explicit Congestion Notification*) dans le champ d'adresse de la trame.

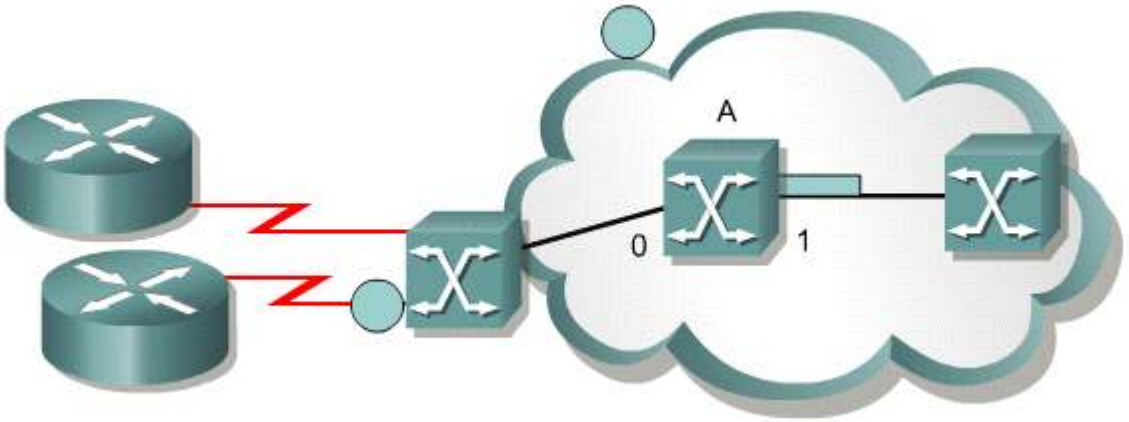
Le bit de notification explicite de congestion au destinataire (FECN – *Forward ECN*) est positionné sur chaque trame reçue par le commutateur sur la liaison encombrée. Le bit de notification explicite de congestion à la source (BECN - *Backward ECN*) est positionné sur chaque trame placée par le commutateur sur la liaison encombrée. Les ETTD qui reçoivent des trames dans lesquelles les bits ECN sont définis sont censés réduire le flux de trames jusqu'à ce que l'encombrement se dissipe. 4

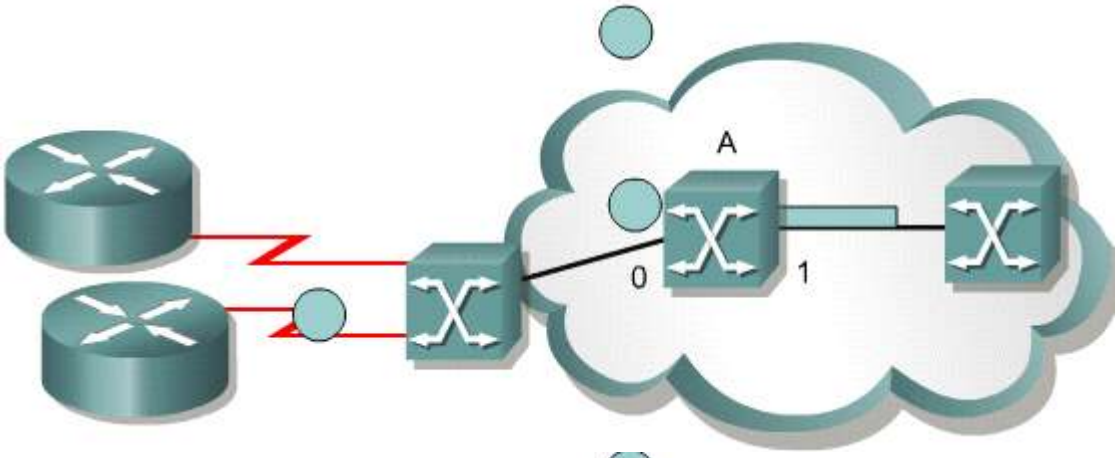


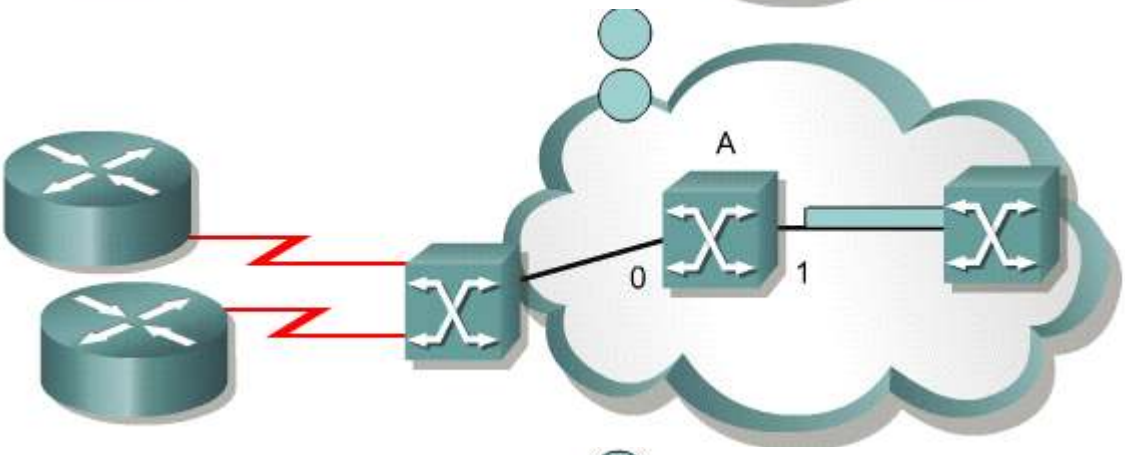
Tandis que le commutateur A place une trame de grande taille sur l'interface 1, les autres trames destinées à cette interface sont mises en file d'attente.

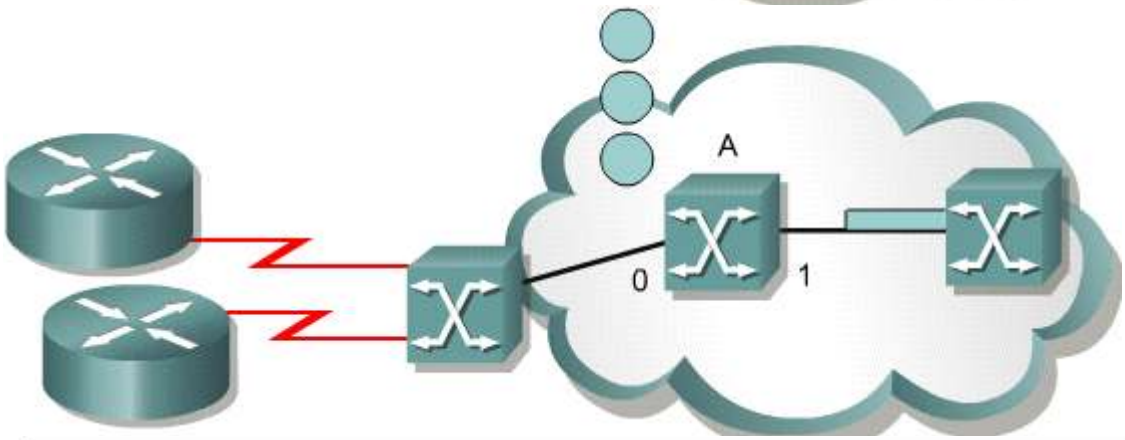




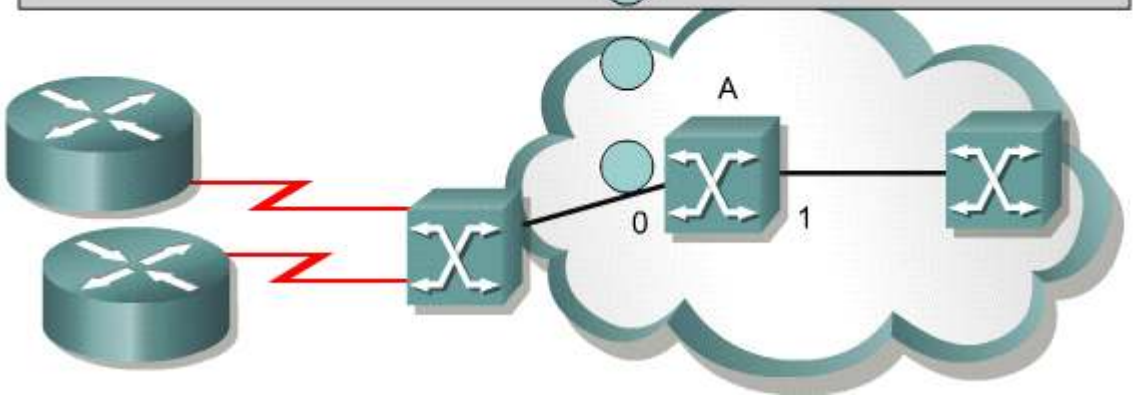




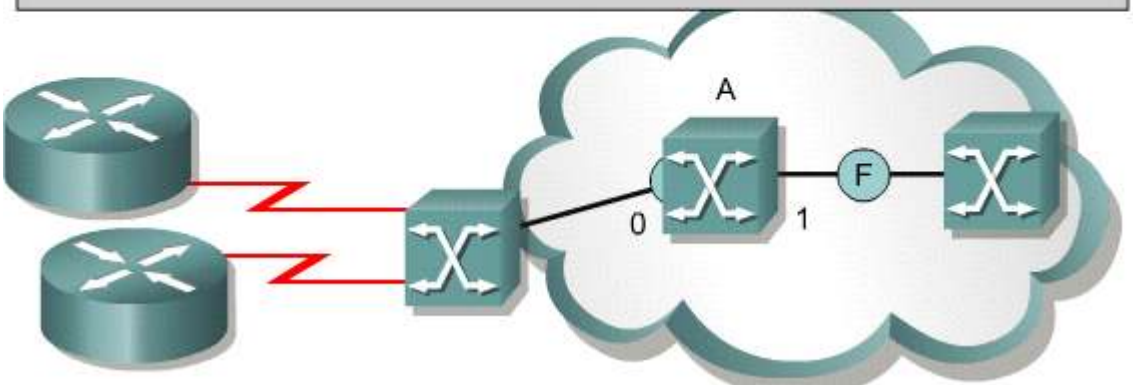




Les équipements en aval sont informés de la file d'attente en configurant le bit FECN (notification explicite de congestion au destinataire).

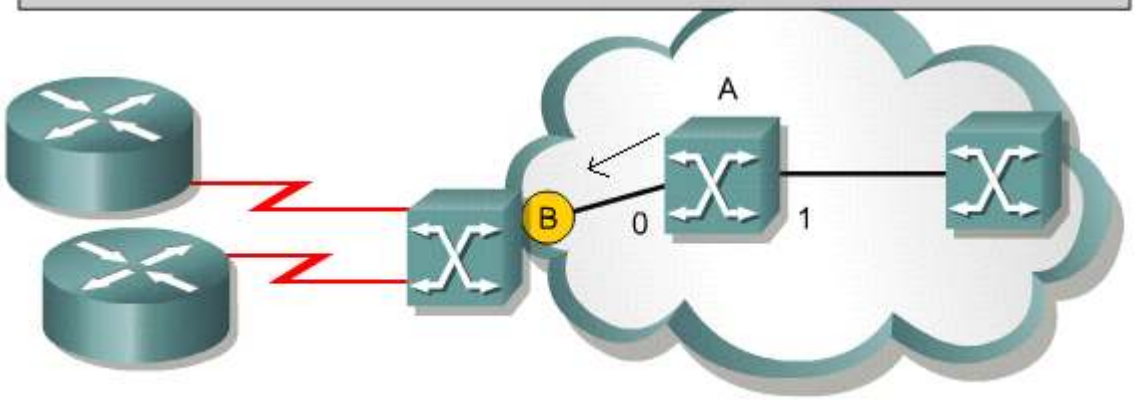


Les équipements en aval sont informés de la file d'attente en configurant le bit FECN (notification explicite de congestion au destinataire).



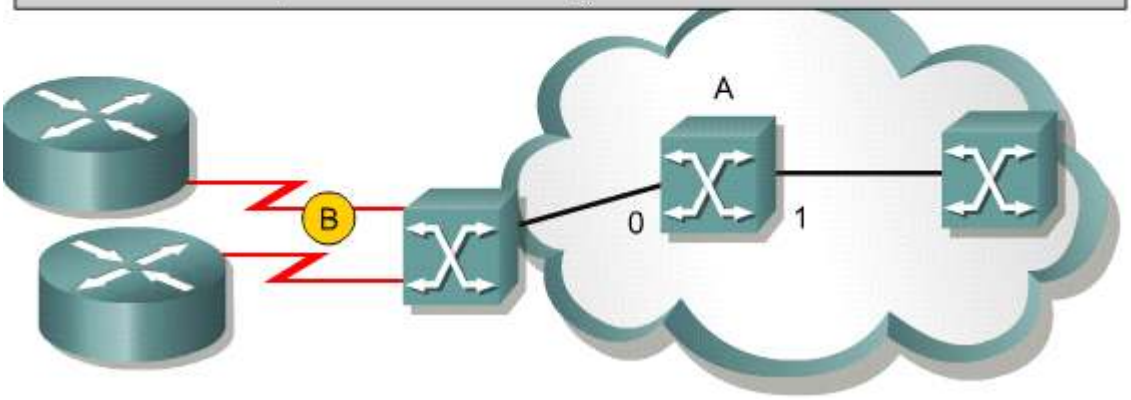
Les équipements en aval sont informés de la file d'attente en configurant le bit FECN (notification explicite de congestion au destinataire).

Les équipements en amont sont informés de la file d'attente en configurant le bit BECN (notification explicite de congestion à la source) ; même s'ils n'ont pas contribué à la congestion.



Les équipements en aval sont informés de la file d'attente en configurant le bit FECN (notification explicite de congestion au destinataire).

Les équipements en amont sont informés de la file d'attente en configurant le bit BECN (notification explicite de congestion à la source) ; même s'ils n'ont pas contribué à la congestion.



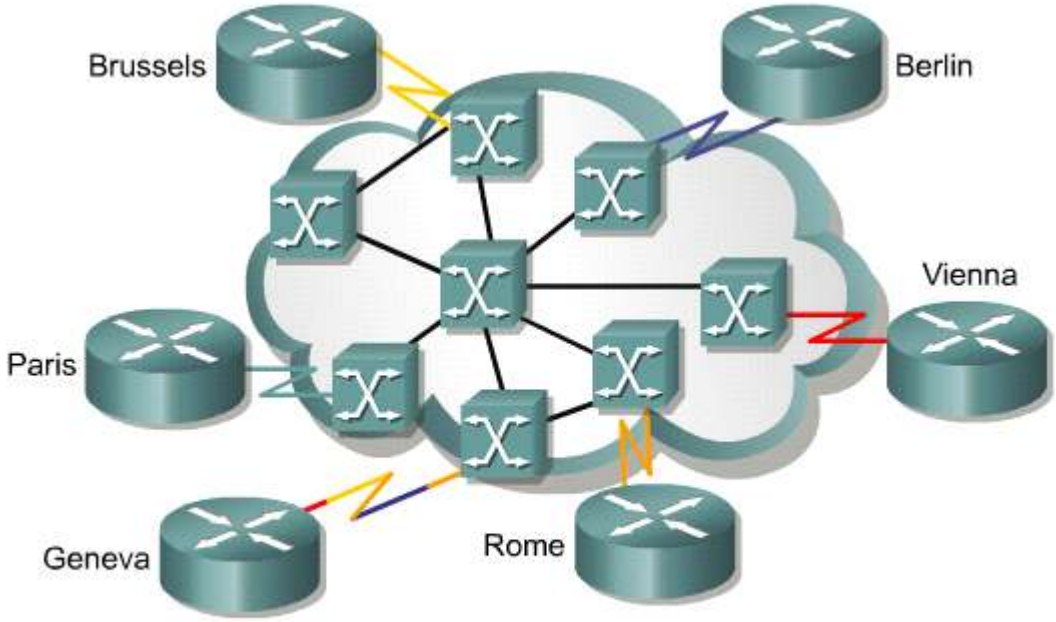
Si l'encombrement se produit sur une agrégation interne, les ETTD peuvent recevoir une notification, même s'ils ne sont pas à l'origine de l'encombrement.

Les bits DE, FECN et BECN font partie du champ d'adresse de la trame LAPF.

Quand plus de deux sites doivent être connectés, il s'avère nécessaire de réfléchir à la topologie des connexions.

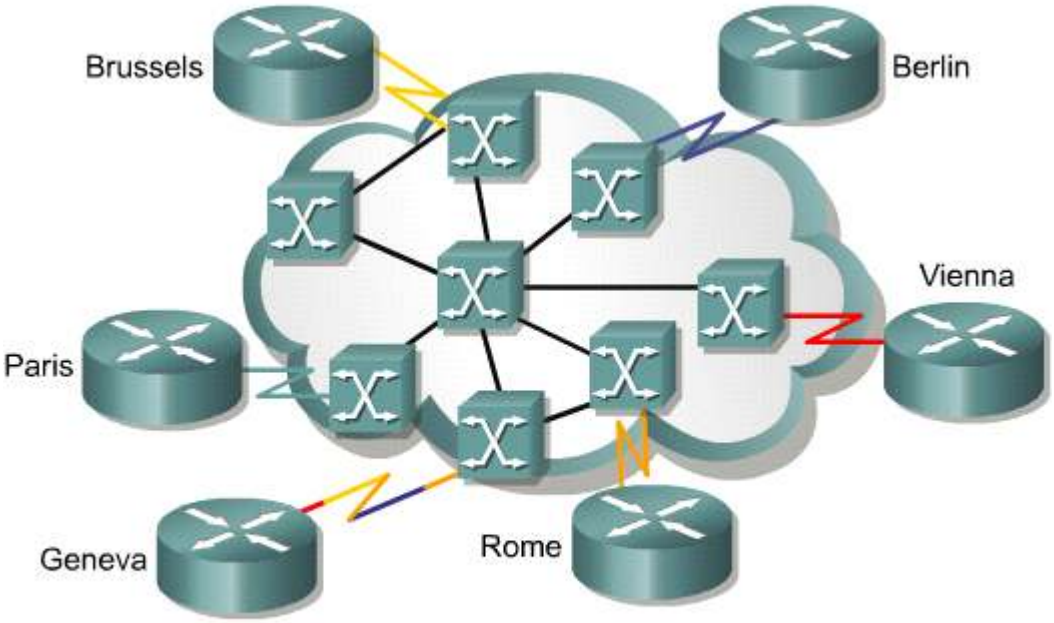
Il est peu probable que Frame Relay soit rentable quand deux sites seulement sont reliés par une connexion point-à-point. Frame Relay est plus rentable quand plusieurs sites doivent être interconnectés.

Les WAN sont souvent interconnectés suivant une topologie en étoile. Un site central héberge les principaux services et est connecté à chaque site distant nécessitant un accès aux services. 1



Topologie en étoile Frame Relay - Hub avec une seule liaison physique et 5 circuits virtuels

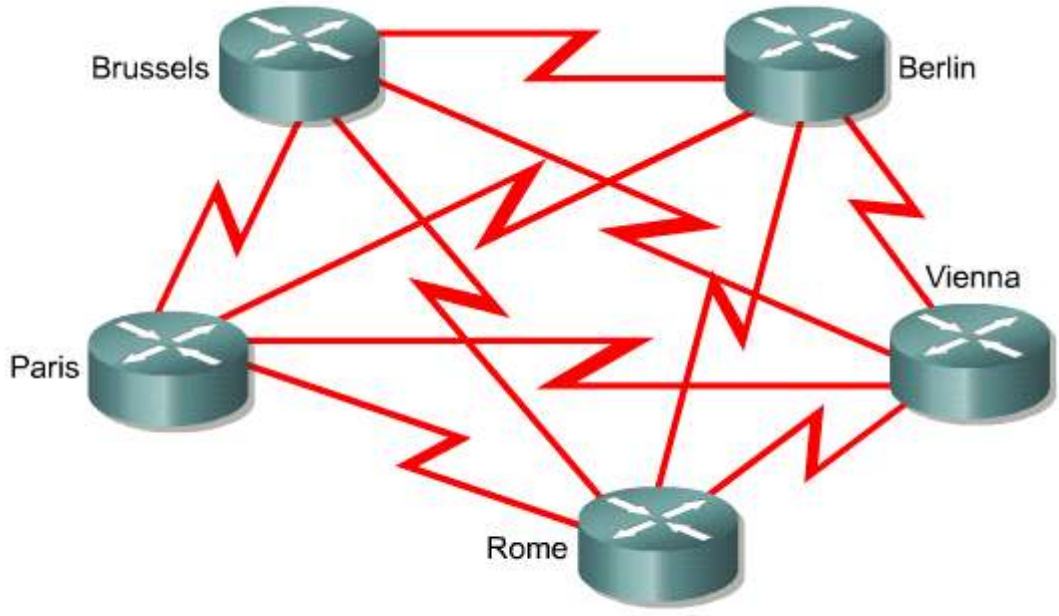
Avec une topologie « hub and spoke », le concentrateur est mis à l'emplacement permettant de réduire au maximum les coûts de la ligne louée. Avec une topologie en étoile pour Frame Relay, chaque site distant dispose d'une liaison d'accès au nuage Frame Relay avec un seul circuit virtuel. Le concentrateur a une liaison d'accès avec plusieurs circuits virtuels, un pour chaque site distant. 2



Topologie en étoile Frame Relay - Hub avec une seule liaison physique et 5 circuits virtuels

Comme les tarifs de Frame Relay ne sont pas assujettis à la distance, il n'est pas nécessaire que le concentrateur se trouve au centre du réseau.

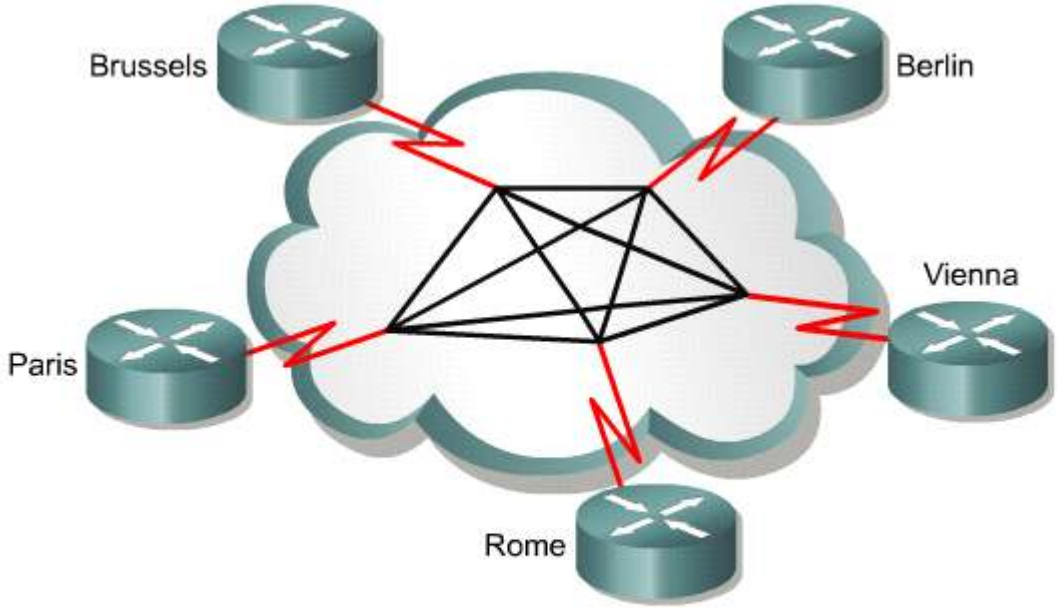
On choisit une topologie en maillage global quand les services à joindre sont dispersés géographiquement et qu'un accès très fiable est nécessaire. Avec le maillage global, chaque site est connecté à tous les autres sites. Contrairement aux interconnexions de lignes louées, Frame Relay ne nécessite aucun matériel supplémentaire. 3



Topologie à maillage global - 5 nœuds nécessitent 10 liaisons

Il est nécessaire de configurer d'autres circuits virtuels sur les liaisons existantes pour passer d'une topologie en étoile à un maillage global. Plusieurs circuits virtuels sur une liaison d'accès exploitent généralement mieux Frame Relay que des VC isolés.

En effet, ils profitent du multiplexage statistique intégré. 4



Topologie maillée - Chaque ETTD possède une liaison physique et 4 circuits virtuels

Pour les réseaux de grande taille, une topologie en maillage global est rarement accessible financièrement. En effet, le nombre de liaisons requises pour ce type de topologie augmente pour pratiquement atteindre le carré du nombre de sites. Même si Frame Relay ne connaît aucun problème lié à l'équipement, chaque liaison est limitée à moins de 1000 circuits virtuels. En pratique, la limite est inférieure à cela et les réseaux plus importants adoptent généralement une topologie en maillage partiel. Avec le maillage partiel, il y a plus d'interconnexions que dans une disposition en étoile, mais pas autant qu'avec un maillage global. L'arrangement effectif dépend beaucoup des besoins en matière de flux de données.

Dans n'importe quelle topologie Frame Relay, quand une seule interface sert à interconnecter plusieurs sites, des problèmes d'accessibilité peuvent survenir. Ceci est dû à la nature d'accès multiple sans diffusion (NBMA - *nonbroadcast multiaccess*) de Frame Relay. «Split horizon» est une technique utilisée par les protocoles de routage pour éviter les boucles de routage. «Split horizon» ne permet pas d'envoyer des mises à jour de routage à partir de l'interface qui était à la source des informations de route. Ceci peut occasionner des problèmes de mise à jour de routage dans un environnement Frame Relay où plusieurs circuits virtuels permanents utilisent une seule interface physique.

Quelle que soit la topologie sous-jacente du réseau physique, il est nécessaire d'effectuer un mappage au niveau de chaque FRAD ou routeur entre une adresse Frame Relay de la couche de liaison de données et une adresse de la couche réseau, par exemple une adresse IP. Fondamentalement, le routeur doit savoir quels réseaux sont accessibles au-delà d'une interface en particulier. Le problème est le même si une ligne louée ordinaire est connectée à une interface. La différence réside dans le fait que l'extrémité distante d'une ligne louée est connectée directement à un seul routeur. Les trames provenant de l'ETTD sont acheminées sur une ligne louée jusqu'au commutateur de réseau, où elles peuvent ensuite se disperser sur jusqu'à 1000 routeurs. L'identificateur DLCI de chaque circuit virtuel doit être associé à l'adresse réseau de son routeur distant. Ces informations peuvent être configurées manuellement à l'aide de commandes de mappage. Le DLCI peut également être configuré automatiquement, au moyen de la résolution d'adresse inverse. Ce processus est présenté en détail dans une section séparée.

5.1 Concepts Frame Relay

5.1.6 LMI Frame Relay

Frame Relay a été conçu pour assurer la transmission de données à commutation de paquets avec un minimum de délais de bout en bout. Tous les éléments risquant de contribuer aux délais ont été omis. Quand les constructeurs ont mis en oeuvre Frame Relay à titre de technologie séparée et non plus de simple composant du RNIS, ils ont décidé qu'il était nécessaire que les ETTD puissent acquérir de façon dynamique des informations sur l'état du réseau. Cette fonctionnalité a été omise dans la conception d'origine. Les extensions nécessaires pour ce transfert de l'état sont appelées l'interface de supervision locale (LMI – *Local Management Interface*).

Le champ DLCI de 10 bits accepte les identificateurs de circuit virtuel de 0 à 1023. Les extensions LMI réservent quelques-uns de ces identificateurs. Ceci réduit le nombre de circuits virtuels autorisés. L'ETTD et l'ETCD s'échangent des messages LMI à l'aide de ces identificateurs DLCI réservés. 1

Identificateurs de circuit virtuel	Types de circuits virtuels
0	LMI (ANSI, ITU)
1..15	Réservé pour une utilisation ultérieure
992..1007	CLLM
1008..1022	Réservé pour une utilisation ultérieure (ANSI, ITU)
1019..1020	Diffusion multicast (Cisco)
1023	LMI (Cisco)

Les extensions LMI incluent les éléments suivants:

- Le mécanisme de test d'activité, qui vérifie qu'un circuit virtuel est opérationnel
- Le mécanisme multicast
- Le contrôle de flux
- La possibilité de donner une signification globale aux identificateurs DLCI
- Le mécanisme d'état du circuit virtuel

Il existe plusieurs types d'interfaces LMI, toutes mutuellement incompatibles. Le type de LMI configuré sur le routeur doit correspondre au type utilisé par l'opérateur. Trois types d'interfaces LMI sont pris en charge par les routeurs Cisco :

- **Cisco** – Les extensions LMI d'origine
- **Ansi** – Correspondant à la norme ANSI T1.617 annexe D
- **q933a** – Correspondant à la norme de l'ITU Q933 annexe A

Les messages LMI sont acheminés dans une variante des trames LAPF. Cette variante inclut quatre champs d'en-tête supplémentaires la rendant compatible avec les trames LAPD utilisées pour le RNIS. Le champ d'adresse achemine l'un des identificateurs DLCI réservés. Il est suivi des champs de contrôle, d'indicateur de protocole et de référence d'appel, qui ne changent pas. Le quatrième champ indique le type de message LMI. 2

Un ou plusieurs éléments d'informations (IE) suivent l'en-tête. Chaque IE contient les éléments suivants:

- Un identificateur d'IE sur un octet
- Un champ de longueur d'IE
- Un ou plusieurs octets contenant des données concrètes, qui incluent généralement l'état d'un identificateur DLCI

Les messages d'état facilitent la vérification de l'intégrité des liaisons logiques et physiques. Ces informations sont cruciales au sein d'un environnement de routage, car les protocoles de routage fondent leurs décisions sur l'intégrité des liaisons.

Activité de média interactive

Glisser-Positionner: Format de message LMI

À la fin de cette activité, l'étudiant sera en mesure d'ordonner correctement les champs d'une trame de message LMI.

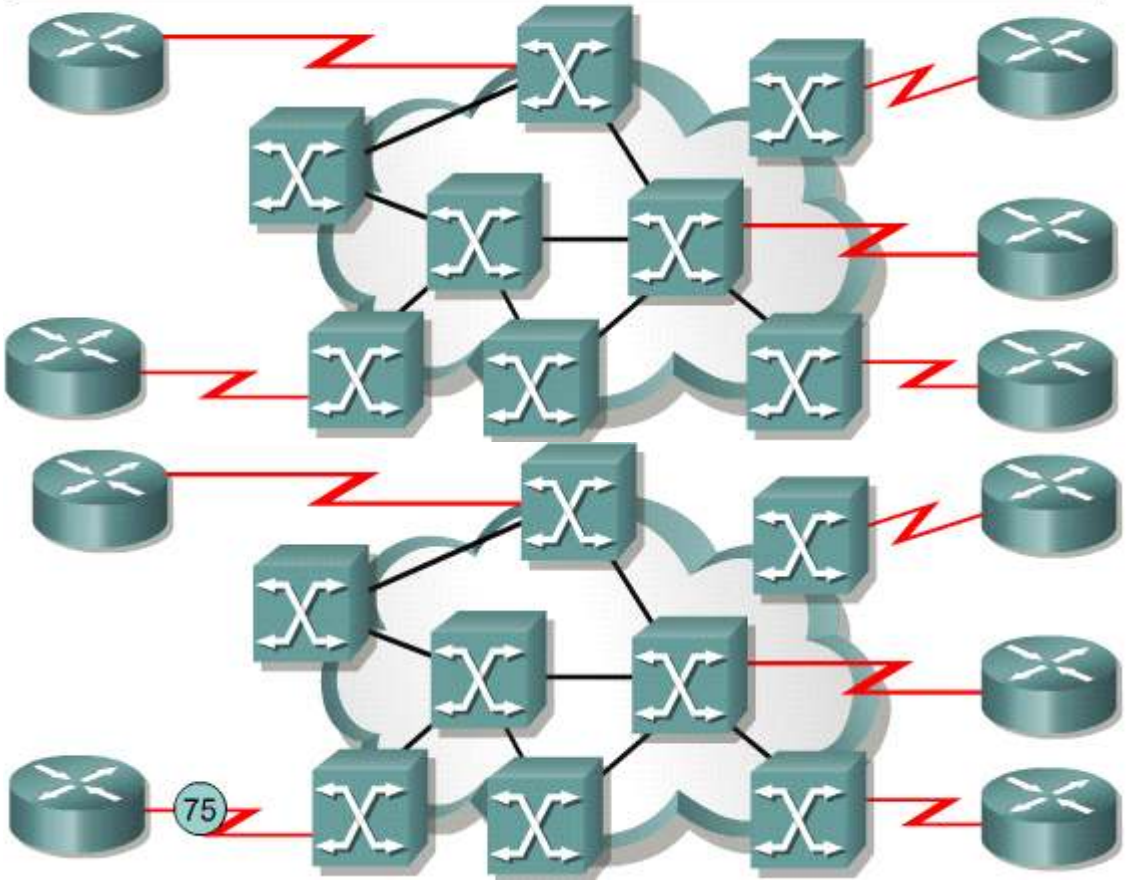
5.1 Concepts Frame Relay

5.1.7 Étapes des protocoles de résolution d'adresse inverse et LMI

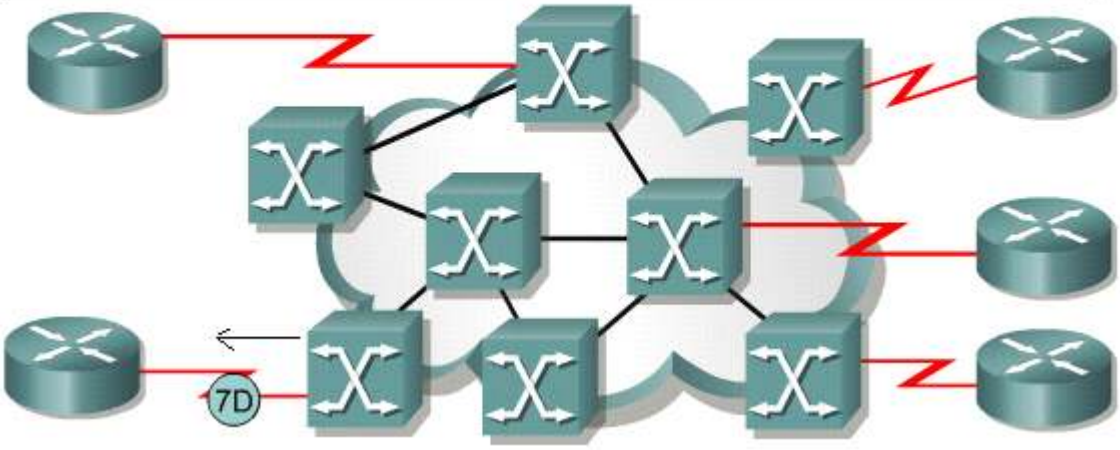
Les messages d'état LMI combinés aux messages du protocole de résolution d'adresse inverse permettent à un routeur d'associer les adresses de la couche réseau et de la couche de liaison de données.

Quand un routeur connecté à un réseau Frame Relay démarre, il envoie au réseau un message d'interrogation de l'état LMI. Le réseau répond par un message d'état LMI contenant des informations sur chaque circuit virtuel configuré sur la liaison d'accès. 1

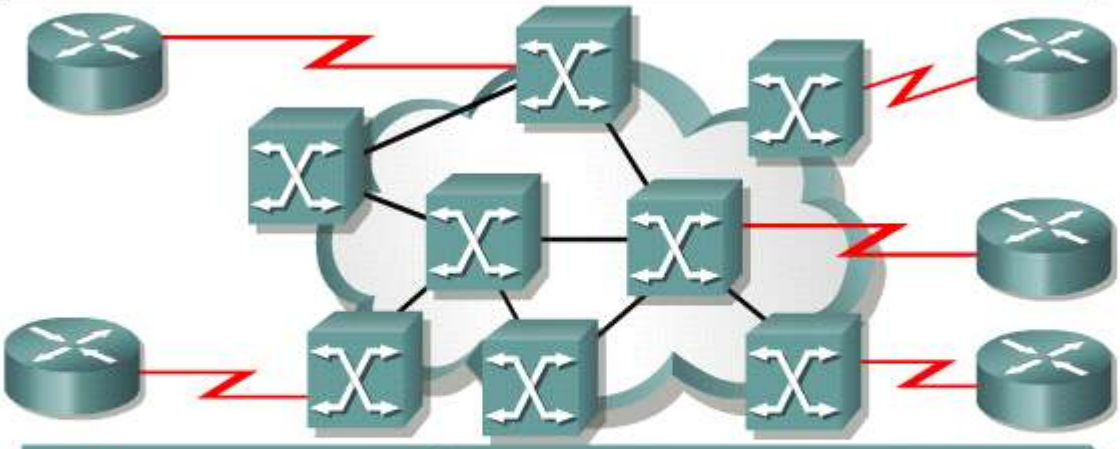
L'ETTD envoie un message d'interrogation d'état (75) à l'ETCD



L'ETTD envoie un message d'interrogation d'état (75) à l'ETCD
L'ETCD répond par un message d'état (7D) qui comprend des identificateurs DLCI configurés



L'ETTD envoie un message d'interrogation d'état (75) à l'ETCD
L'ETCD répond par un message d'état (7D) qui comprend des identificateurs DLCI configurés
L'ETCD est informé des circuits virtuels dont il dispose

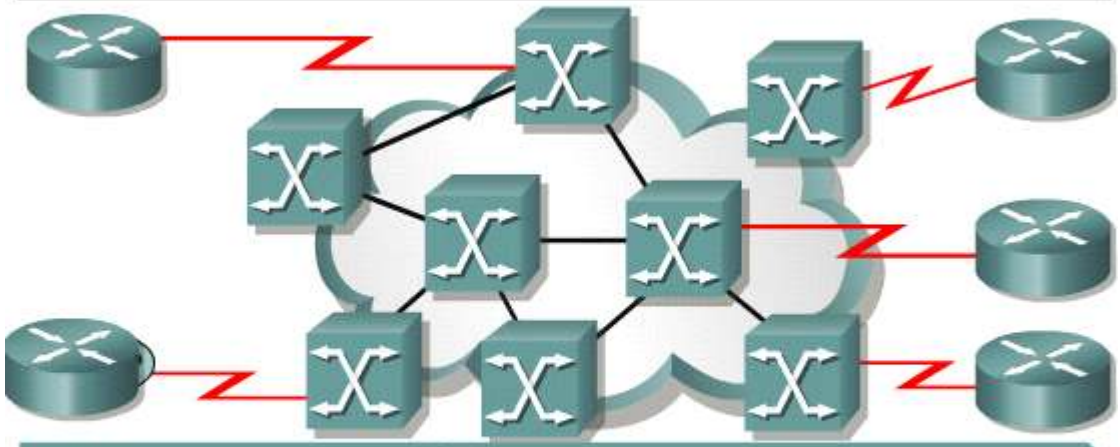


DLCI	État
101	Actif
102	Actif
103	Actif
104	Actif

Le routeur répète régulièrement cette interrogation de l'état, mais les réponses ultérieures n'incluent que les changements d'état. Après un nombre prédéfini de ces réponses abrégées, le réseau envoie un message d'état complet.

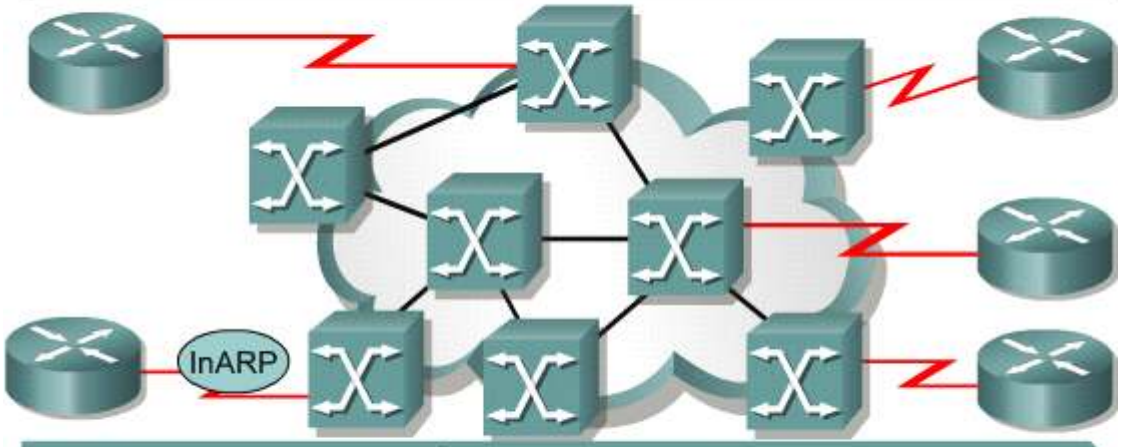
Si le routeur doit mapper les circuits virtuels à des adresses de la couche réseau, il envoie un message de résolution d'adresse inverse sur chaque circuit virtuel. Ce message contient l'adresse de couche réseau du routeur, afin que l'ETTD ou le routeur distant puisse également procéder au mappage. La réponse de résolution d'adresse inverse permet au routeur d'inscrire les entrées de mappage nécessaires dans sa table de correspondances adresse-DLCI. Si plusieurs protocoles de couche réseau sont pris en charge par la liaison, des messages de résolution d'adresse inverse sont renvoyés pour chacun d'entre eux. 2

L'ETTD envoie un protocole de résolution d'adresse inverse à l'adresse réseau sur un circuit virtuel VCMapping



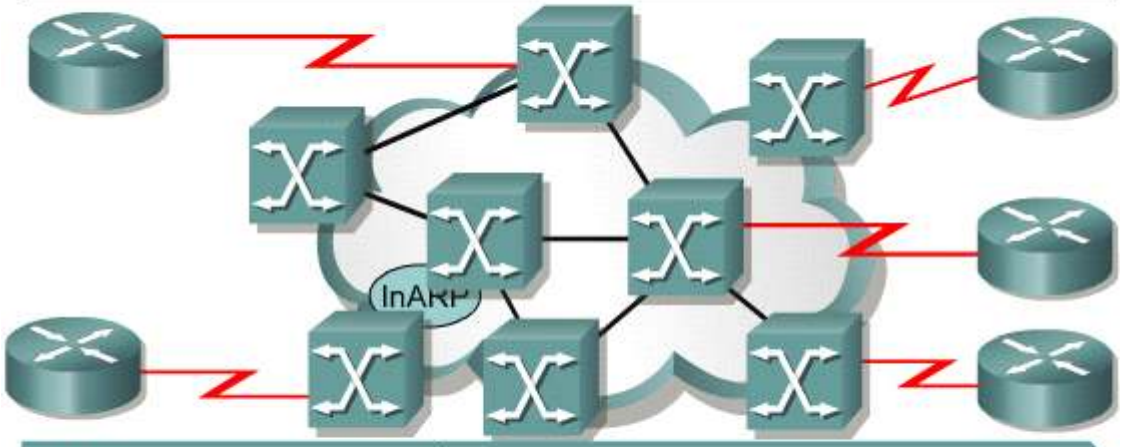
DLCI	État
101	Actif
102	Actif
103	Actif
104	Actif

L'ETTD envoie un protocole de résolution d'adresse inverse à l'adresse réseau sur un circuit virtuel VCMapping

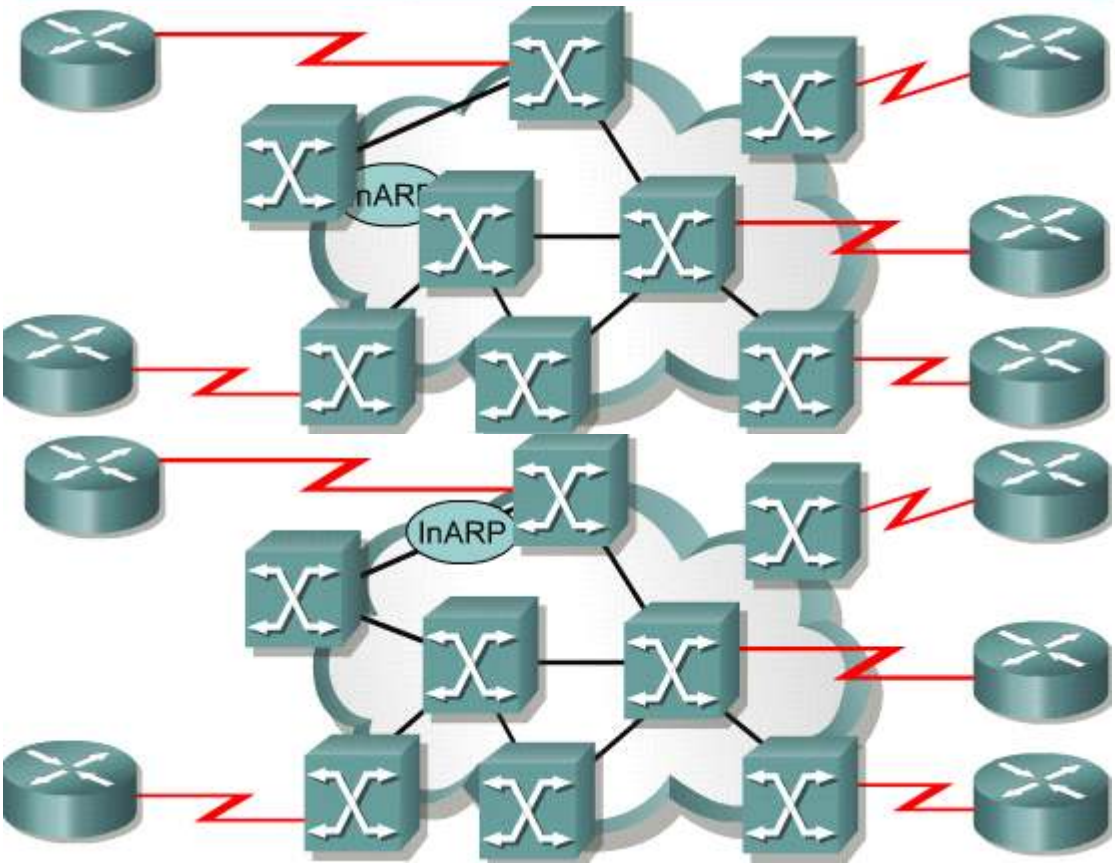


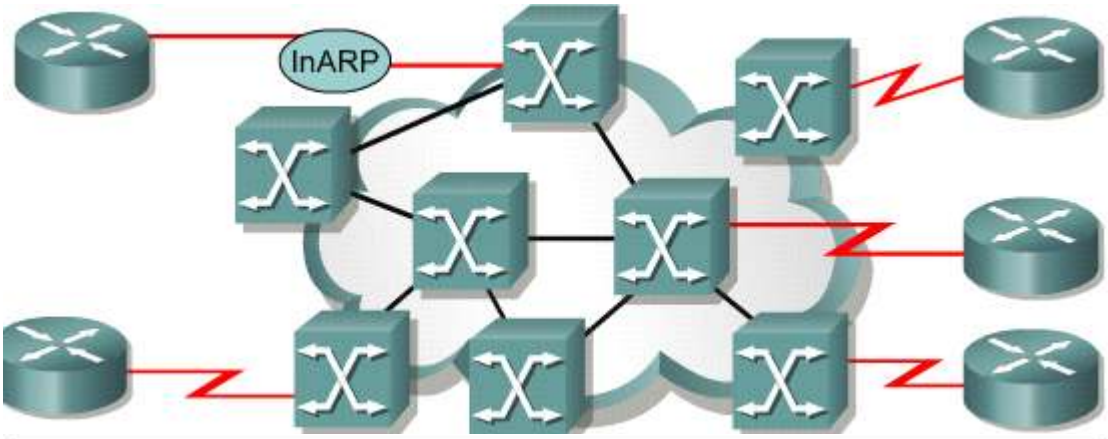
DLCI	État
101	Actif
102	Actif
103	Actif
104	Actif

L'ETTD envoie un protocole de résolution d'adresse inverse à l'adresse réseau sur un circuit virtuel VCMapping



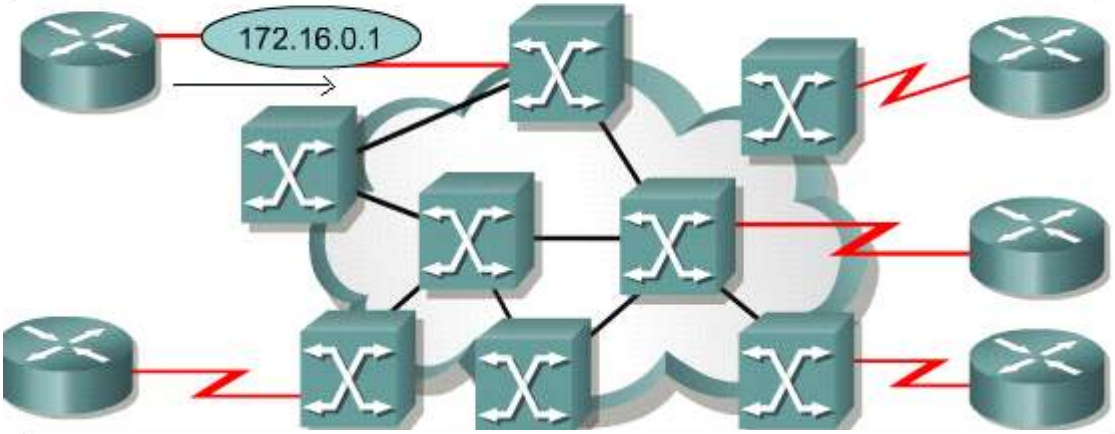
DLCI	État
101	Actif
102	Actif
103	Actif
104	Actif





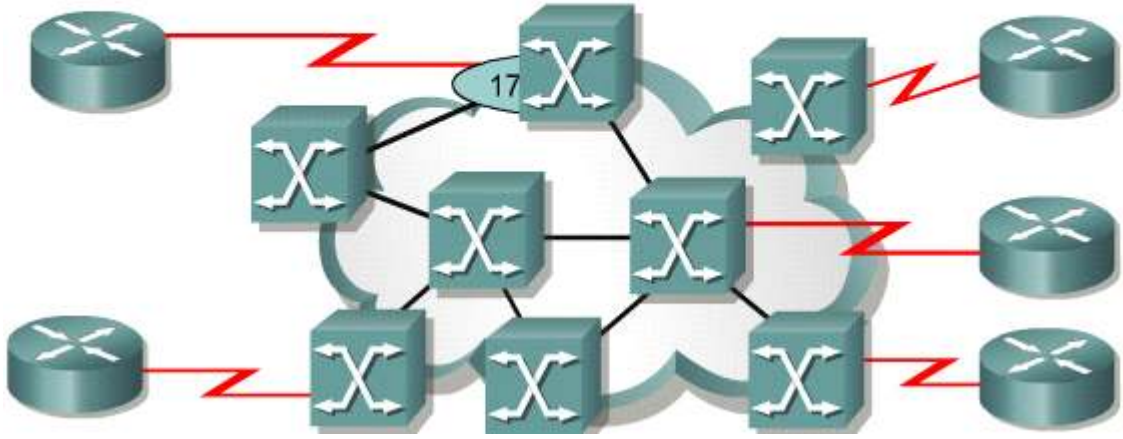
L'ETTD envoie un protocole de résolution d'adresse inverse à l'adresse réseau sur un circuit virtuel VCMapping

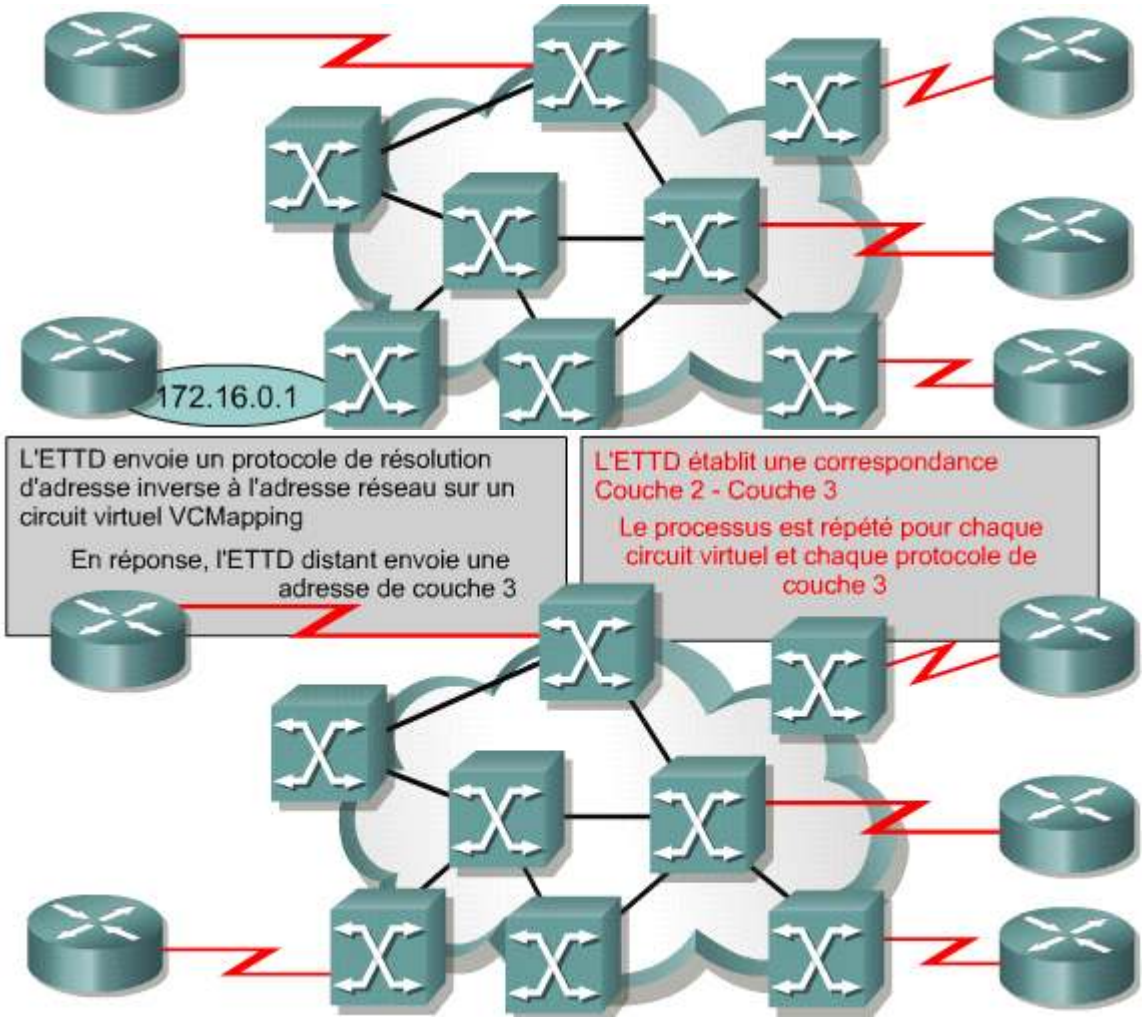
En réponse, l'ETTD distant envoie une adresse de couche 3



L'ETTD envoie un protocole de résolution d'adresse inverse à l'adresse réseau sur un circuit virtuel VCMapping

En réponse, l'ETTD distant envoie une adresse de couche 3

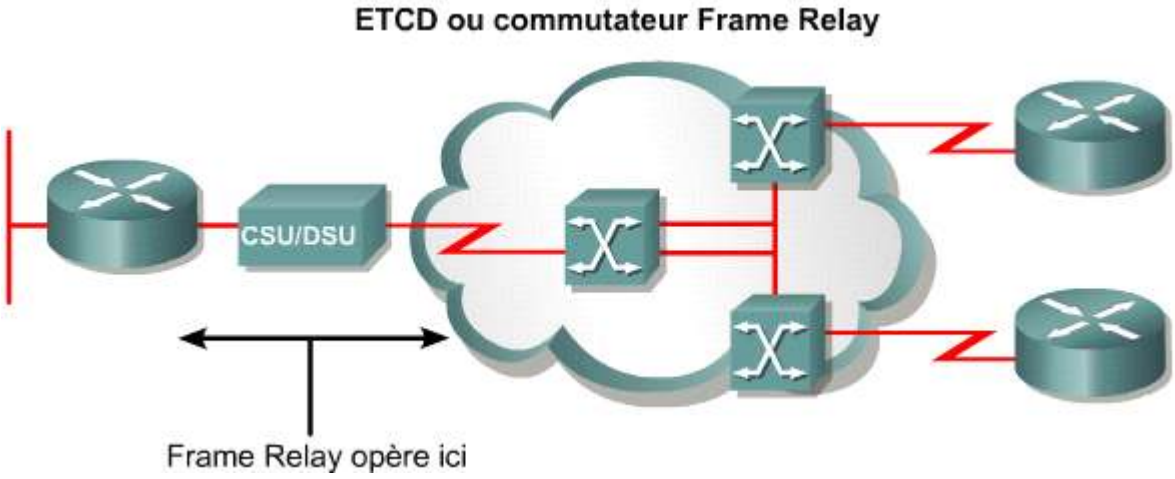



172.16.0.1
L'ETTD envoie un protocole de résolution d'adresse inverse à l'adresse réseau sur un circuit virtuel VCMapping
En réponse, l'ETTD distant envoie une adresse de couche 3
L'ETTD établit une correspondance Couche 2 - Couche 3
Le processus est répété pour chaque circuit virtuel et chaque protocole de couche 3

5.2 Configuration de Frame Relay

5.2.1 Configuration de base de Frame Relay

La présente section décrit la configuration de base d'un circuit virtuel permanent Frame Relay. 1



Frame Relay est configuré sur une interface série. Le type d'encapsulation par défaut est celui de la version propriétaire Cisco de HDLC. Pour passer à l'encapsulation Frame Relay, utilisez la commande **`encapsulation frame-relay [cisco | ietf]`**.

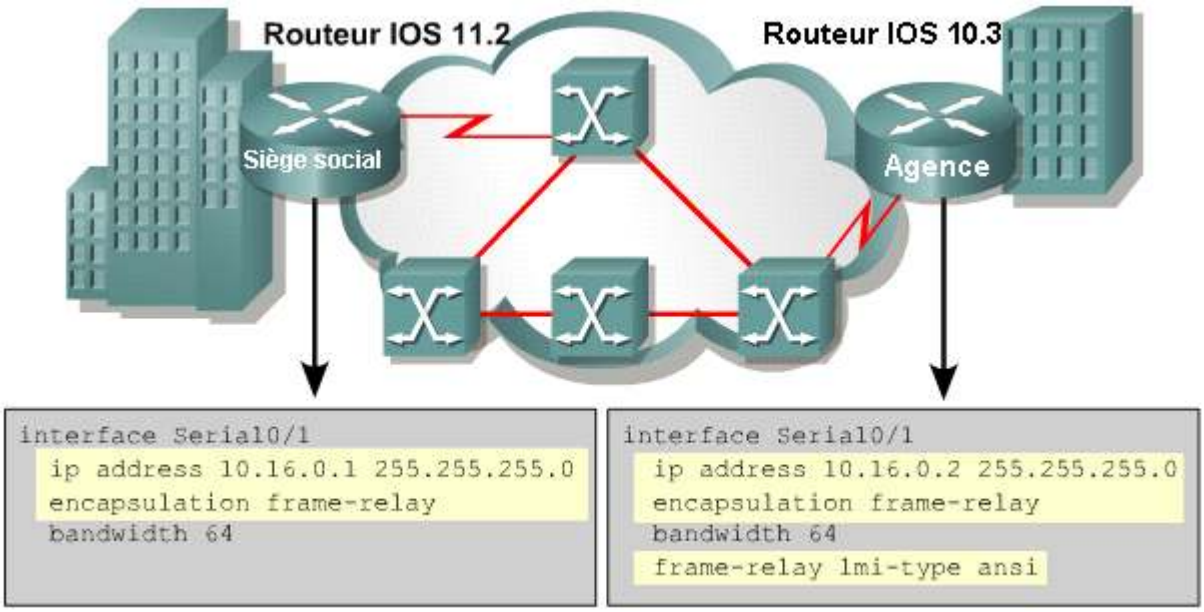
`cisco` Utilise l'encapsulation Frame Relay propriétaire de Cisco. Utilisez cette option pour effectuer une connexion à un autre routeur Cisco. De nombreux équipements non-Cisco prennent également en charge ce type d'encapsulation. Il s'agit de la valeur par défaut.

`ietf` Rend la méthode d'encapsulation à la norme RFC 1490 de l'IETF (*Engineering Task Force*). Sélectionnez cette option si

vous vous connectez à un routeur non-Cisco.

L'encapsulation Frame Relay propriétaire de Cisco fait appel à un en-tête sur 4 octets, dont 2 désignent l'identificateur de connexion de liaisons de données (DLCI) et 2 le type de paquet.

Définissez une adresse IP pour l'interface au moyen de la commande **`ip address`**. Définissez la bande passante de l'interface série à l'aide de la commande **`bandwidth`**. La bande passante se spécifie en kilobits par seconde (kbits/s). Cette commande sert à avertir le protocole de routage que la bande passante est configurée de façon statique sur la liaison. La valeur de bande passante est utilisée par les protocoles IGRP (*Interior Gateway Routing Protocol*), EIGRP (*Enhanced Interior Gateway Routing Protocol*) et OSPF (*Open Shortest Path First*) pour déterminer la métrique de la liaison. 2



La commande **`frame-relay lmi-type [ansi | cisco | q933a]`** permet d'établir et de configurer la connexion LMI. Cette commande est seulement nécessaire avec la plate-forme logicielle Cisco IOS 11.1 ou une version précédente. À partir de l'IOS version 11.2, aucune configuration n'est nécessaire, car le type de LMI est détecté automatiquement. Cisco est le type de LMI par défaut. Le type de LMI se définit en fonction de l'interface. Il est renvoyé par la commande **`show interfaces`**.

Les étapes de configuration sont les mêmes, quels que soient les protocoles de couche réseau actifs sur le réseau.

Activité de TP

Exercice: Configuration de Frame Relay

Au cours de ce TP, l'étudiant va configurer un routeur afin d'établir une connexion vers un commutateur Frame Relay local.

Activité de TP

Activité en ligne: Configuration de Frame Relay

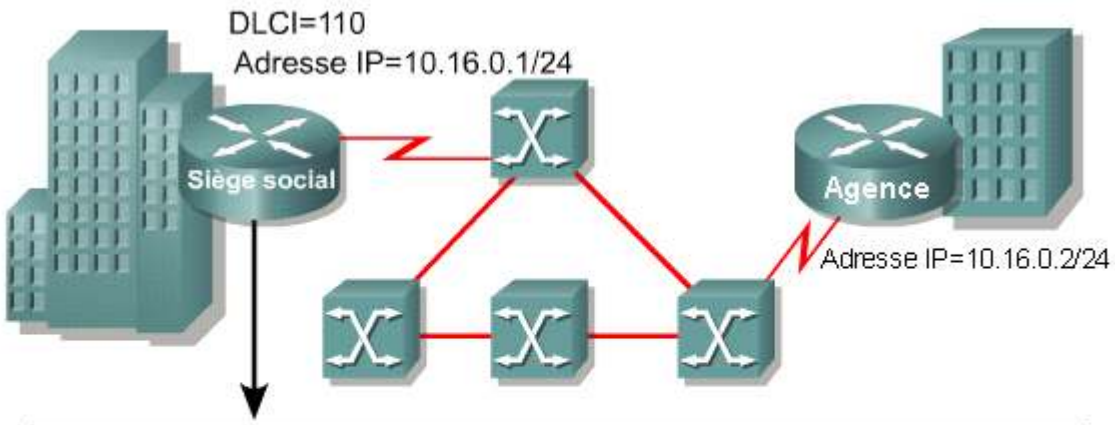
Au cours de ce TP, un routeur va être configuré pour établir une connexion vers un commutateur Frame Relay local.

5.2 Configuration de Frame Relay

5.2.2 Configuration d'une carte Frame Relay statique

L'identificateur DLCI doit être mappé de façon statique à l'adresse de couche réseau du routeur distant quand ce dernier ne prend pas en charge la résolution d'adresse inverse. Ceci est également vrai quand le trafic de diffusion broadcast et multicast doit être contrôlé sur le circuit virtuel permanent. Ces entrées de carte Frame Relay statiques sont désignées par le nom de cartes statiques.

Utilisez la commande **`frame-relay map protocol protocol-address dlci [broadcast]`** pour mapper de façon statique l'adresse de couche réseau à l'identificateur DLCI local. 1 – 2




```
interface Serial 0/1
  ip address 10.16.0.1 255.255.255.0
  encapsulation frame-relay
  bandwidth 64
  frame-relay map ip 10.16.0.2 110 broadcast
```

Paramètres de la commande	Description
protocol	Définit le protocole, le pontage ou le contrôle de lien logique pris en charge : appletalk, decnet, dlsw, ip, ipx, llc2, rsrb, vines et xns.
protocol-address	Définit l'adresse de couche réseau de l'interface du routeur de destination.
dlci	Définit l'identificateur DLCI local utilisé pour la connexion à l'adresse de protocole distante.
broadcast	(Facultatif) Permet la diffusion de broadcasts et de multicasts sur le circuit virtuel, d'où la possibilité d'utiliser des protocoles de routage dynamique sur le circuit virtuel.

Activité de TP

Exercice: Configuration d'un circuit virtuel permanent Frame Relay

Au cours de ce TP, l'étudiant va configurer deux routeurs successifs pour constituer un circuit virtuel permanent (PVC) Frame Relay.

Activité de TP

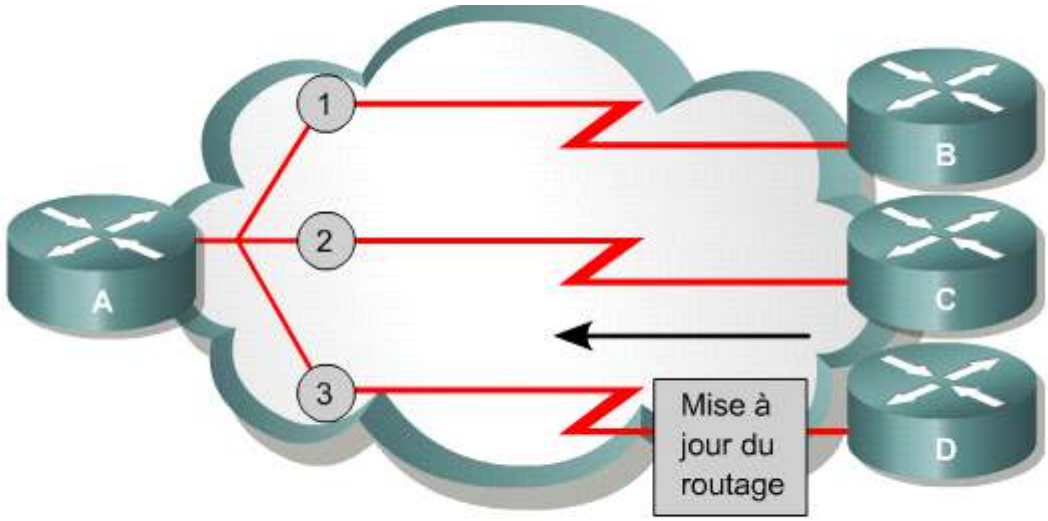
Activité en ligne: show frame-relay map

Au cours de cette activité, l'étudiant va apprendre comment utiliser la commande **`show frame-relay map`** pour afficher les entrées de la carte et des informations sur les connexions.

5.2 Configuration de Frame Relay

5.2.3 Problèmes d'accessibilité relatifs aux mises à jour de routage dans un accès multiple sans diffusion

Par défaut, un réseau Frame Relay fournit une connectivité d'accès multiple sans diffusion (NBMA) entre des sites distants. Un environnement NBMA est considéré comme d'autres environnements de média à accès multiples, tels qu'Ethernet, dans lesquels tous les routeurs sont sur le même sous-réseau. Toutefois, pour réduire les coûts, les nuages NBMA présentent généralement une topologie en étoile «hub-and-spoke». Avec «hub-and-spoke», la topologie physique n'offre pas les capacités d'accès multiples d'Ethernet. 1



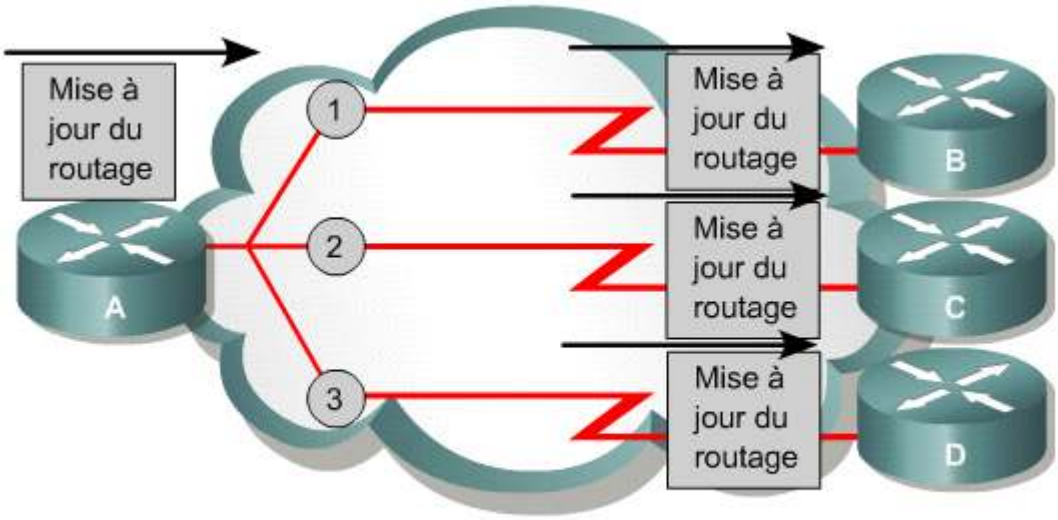
Problème : la mise à jour reçue sur l'interface physique n'est pas retransmise vers cette même interface : " split-horizon "

La topologie physique consiste en plusieurs circuits virtuels permanents.

Une topologie NBMA Frame Relay peut être à l'origine de deux problèmes:

- Problèmes d'accessibilité relatif aux mises à jour de routage
- Le besoin de répliquer les broadcasts sur chaque circuit virtuel permanent lorsqu'une interface physique en contient plusieurs

Les mises à jour «split horizon» réduisent les boucles de routage en empêchant une mise à jour de routage reçue sur une interface physique d'être retransmise par la même interface. Si le routeur B, un routeur « de rayon » diffuse par broadcast une mise à jour de routage au routeur A, le routeur «de moyeu», et que le routeur A dispose de plusieurs circuits virtuels permanents sur une interface physique unique, il ne peut alors pas transférer cette mise à jour de routage vers d'autres routeurs « de rayon » par la même interface physique. Si le «split-horizon» est désactivé, la mise à jour de routage peut être transférée par l'interface physique qu'elle a empruntée pour arriver. «Split-horizon» ne constitue pas un problème quand il n'y a qu'un circuit virtuel permanent sur une interface physique. En effet, il s'agit alors d'une connexion point-à-point Frame Relay. 2



Problème : le trafic de broadcast doit être reproduit pour chaque connexion active

Les routeurs qui prennent en charge plusieurs connexions sur une seule interface physique ont de nombreux circuits virtuels permanents qui se terminent au routeur. Ces routeurs doivent répliquer les paquets de broadcast, tels que les broadcasts de mise à jour de routage, sur chaque circuit virtuel, pour atteindre les routeurs distants. Les paquets de broadcast répliqués peuvent consommer de la bande passante et occasionner une latence significative du trafic utilisateur. Il peut sembler logique de désactiver le « split-horizon » pour résoudre les problèmes d'accessibilité que cette fonction occasionne. Toutefois, certains protocoles de couche réseau n'autorisent pas la désactivation de la fonction « split-horizon », laquelle augmente de toute façon les risques de boucles de routage sur n'importe quel réseau.

Pour résoudre le problème de «split-horizon», une méthode consiste à utiliser une topologie de maillage global. En revanche, cela augmente le coût, car un plus grand nombre de circuits virtuels permanents est alors nécessaire. La meilleure solution consiste à utiliser des sous-interfaces.

5.2 Configuration de Frame Relay

5.2.4 Sous-interfaces Frame Relay

Pour activer le transfert de mises à jour de routage par broadcast dans une topologie Frame Relay «hub-and-spoke», configurez le routeur central avec des interfaces attribuées de manière logique. Ces interfaces sont appelées des sous-interfaces. Les sous-interfaces sont des subdivisions logiques d'une interface physique. [1]

Point-à-point
- Les sous-interfaces font office de lignes louées
- Chaque sous-interface point-à-point a besoin de son propre sous-réseau
- Applicable aux topologies de type " hub-and-spoke "

Multipoint
- Les sous-interfaces font office de réseaux NMBA. Elles ne résolvent donc pas le problème de " split-horizon "
- L'utilisation d'un seul sous-réseau permet d'économiser de l'espace d'adressage
- Applicable aux topologies à maillage partiel et à maillage global

Dans les environnements de routage « split-horizon », les mises à jour de routage reçues au niveau d'une sous-interface peuvent être envoyées à une autre sous-interface. Dans une configuration de sous-interface, chaque circuit virtuel peut être configuré comme une connexion point-à-point. Ceci permet à chaque sous-interface de fonctionner comme une ligne louée. Avec une sous-interface point-à-point Frame Relay, chaque paire de routeurs point-à-point réside dans son propre sous-réseau.

Les sous-interfaces Frame Relay peuvent être configurées en mode point-à-point ou multipoint :

- **Point-à-point** – Une sous-interface point-à-point sert à établir une connexion par circuit virtuel permanent à une interface physique ou à une sous-interface d'un routeur distant. Dans ce cas, chaque paire de routeurs point-à-point

réside sur son propre sous-réseau et chaque sous-interface point-à-point ne dispose que d'un identificateur DLCI. Dans un environnement point-à-point, chaque sous-interface agit comme une interface point-à-point. Par conséquent, le trafic des mises à jour de routage n'est pas soumis à la règle du «split-horizon».

- **Multipoint** – Une sous-interface multipoint sert à établir plusieurs connexions par circuit virtuel permanent vers plusieurs interfaces physiques ou sous-interfaces sur des routeurs distants. Toutes les interfaces participantes se trouvent dans le même sous-réseau. La sous-interface fonctionne comme une interface Frame Relay NBMA, de telle sorte que le trafic des mises à jour de routage est soumis à la règle du «split-horizon».

La commande **`encapsulation frame-relay`** s'applique à l'interface physique. Tous les autres éléments de configuration, tels que l'adresse de couche réseau et les identificateurs DLCI, sont appliqués à la sous-interface.

Des configurations multipoint peuvent être utilisées pour économiser les adresses, particulièrement si aucun masque de sous-réseau de longueur variable (VLSM) n'est utilisé. Toutefois, les configurations multipoints risquent de ne pas fonctionner correctement, compte tenu du trafic de broadcast et du «split-horizon». L'option de sous-interface point-à-point a été créée pour éviter ces problèmes.

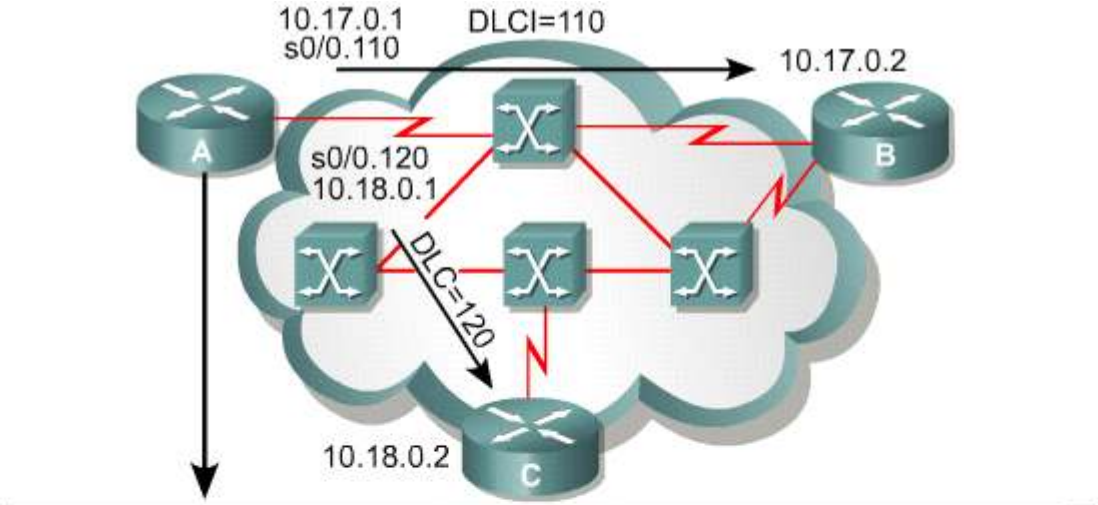
5.2 Configuration de Frame Relay

5.2.5 Configuration de sous-interfaces Frame Relay

C'est l'opérateur Frame Relay qui attribue les numéros d'identification DLCI. Ces numéros vont de 16 à 992, et n'ont généralement qu'une signification locale. Les identificateurs DLCI peuvent avoir une importance globale dans certaines circonstances. Cette plage de numéros est variable, en fonction de l'interface LMI utilisée.

Dans l'illustration, le routeur A comporte deux sous-interfaces point-à-point. La sous-interface s0/0.110 se connecte au routeur B et la sous-interface s0/0.120 au routeur C. Chaque sous-interface réside sur un sous-réseau différent. Pour configurer les sous-interfaces d'une interface physique, procédez comme suit :

- Configurez l'encapsulation Frame Relay sur l'interface physique au moyen de la commande **`encapsulation frame-relay`**
- Pour chacun des circuits virtuels permanents définis, créez une sous-interface logique 1




```
interface Serial0/0
  no ip address
  encapsulation frame-relay
  !
  interface Serial0/0.110 point-to-point
   ip address 10.17.0.1 255.255.255.0
   bandwidth 64
   frame-relay interface-dlci 110
  !
  interface Serial0/0.120 point-to-point
   ip address 10.18.0.1 255.255.255.0
   bandwidth 64
   frame-relay interface-dci 120
  !
```

router(config-if)#**interface serial number.***subinterface-number* [**multipoint** | **point-to-point**] 2

Paramètres de la commande interface serial	Description
subinterface-number	Numéro de sous-interface compris entre 1 et 4294967293. Le numéro de l'interface précédant le point doit être le numéro de l'interface à laquelle appartient la sous-interface.
multipoint	Sélectionnez ce paramètre si tous les routeurs se trouvent dans le même sous-réseau.
point-to-point	Sélectionnez ce paramètre si vous souhaitez que chaque paire de routeurs point-à-point possède son propre sous-réseau. En règle générale, les liaisons point-à-point utilisent le masque de sous-réseau 255.255.255.252

Pour créer une sous-interface, utilisez la commande **interface serial**. Indiquez le numéro de port, suivi d'un point (.), puis du numéro de la sous-interface. En général, le numéro de sous-interface est celui de l'identificateur DLCI. Ceci facilite le dépannage. Le dernier paramètre obligatoire indique si la sous-interface est de type point-à-point ou point-à-multipoint. Le mot clé **multipoint** ou **point-to-point** s'avère alors nécessaire. Il n'y a pas de valeur par défaut. Les commandes suivantes créent la sous-interface du circuit virtuel permanent vers le routeur B :

```
routerA(config-if)#interface serial 0/0.110 point-to-point
```

Si la sous-interface est configurée en point-to-point, l'identificateur DLCI local de la sous-interface doit également être configuré afin que celle-ci puisse être distinguée de l'interface physique. Le DLCI est également nécessaire pour les sous-interfaces

multipoint pour lesquelles la résolution d'adresse inverse a été activée. Il n'est pas obligatoire pour les sous-interfaces multipoint configurées avec des correspondances de route statiques. La commande **frame-relayinterface-dlci** sert à configurer l'identificateur DLCI local sur la sous-interface.

`router(config-subif)#`**`frame-relay interface-dlci`***`dlci-number`* 3

Paramètre de la commande frame-relay interface-dlci	Description
dlci-number	Définit l'identificateur DLCI en cours de connexion à la sous-interface. C'est la seule façon de lier un identificateur DLCI LMI à une sous-interface, car l'Interface de Supervision Locale ne connaît pas les sous-interfaces. Utilisez la commande frame-relay interface-dlci uniquement sur des sous-interfaces.

Activité de TP

Exercice: Configuration de sous-interfaces Frame Relay

Au cours de ce TP, l'étudiant va configurer trois routeurs sur un réseau Frame Relay à maillage global.

Activité de TP

Activité en ligne: Configuration de sous-interfaces Frame Relay

Au cours de cette activité, l'étudiant va configurer trois routeurs sur un réseau Frame Relay à maillage global.

5.2 Configuration de Frame Relay

5.2.6 Vérification de la configuration Frame Relay

La commande **show interfaces** affiche des informations sur l'encapsulation et l'état des couches 1 et 2. Elle affiche également les informations ci-dessous:

- Le type d'interface LMI
- L'identificateur DLCI de l'interface LMI
- Le type d'équipement terminal de traitement de données/équipement de terminaison de circuit de données (ETTD/ETCD)

Généralement, le routeur est considéré comme un équipement terminal de traitement de données (ETTD). Toutefois, il est possible de configurer un routeur Cisco comme commutateur Frame Relay. Le routeur devient un équipement de terminaison de circuit de données (ETCD) quand il est configuré en tant que commutateur Frame Relay. 1

```
Router#show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 150 bytes, BW 1544 Kbit, DLY 20000 usec, relay
  255/255, load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive
  set (10 sec)
  LMI enq sent 19, LMI stat recvd 20, LMI upd recvd 0,
  DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 8/0,
  interface broadcasts 5
  Last clearing of "show interface" counters never
  Queueing startagy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, o drops
  <Output omitted>
```

Utilisez la commande **`show frame-relay lmi`** pour afficher les statistiques relatives au trafic sur l'interface LMI. 2

```
Router#show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE)
LMI TYPE = CISCO
  Invalid Unnumbered info 0 Invalid Prot Disc 0
  Invalid dummy Call Ref 0 Invalid Msg Type 0
  Invalid Status Message 0 Invalid Lock Shift 0
  Invalid Information ID 0 Invalid Report IE Len 0
  Invalid Report Request 0 Invalid Keep IE Len 0
  Num Status Enq. Sent 113100 Num Status msgs Rcvd
  113100
  Num Update Status Revd 0 Num Status Timeouts 0
```

Par exemple, cette commande montre le nombre de messages d'état échangés entre le routeur local et le commutateur Frame Relay local.

Utilisez la commande **`show frame-relay pvc [interface interface] [dlci]`** pour afficher l'état de chaque circuit virtuel permanent configuré, ainsi que des statistiques sur le trafic. 3

```
Router#show frame-relay pvc 100

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI - 100, DLCI USAGE - LOCAL, PVC STATUS - ACTIVE,
INTERFACE - Serial0/0

 input pkts 28      output pkts 10      in bytes 8398
 out bytes 1198     dropped pkts 0      in FECN pkts 0
 in BECN pkts 0     out FECN pkts 0     out BECN pkts 0
 in DE pkts 0       out DE pkts 0
 out bcast pkts 10 out bcast bytes 1198
 pvc create time 00:03:46, last time pvc status changed
 00:03:47
```

Cette commande s'avère également utile pour afficher le nombre de paquets BECN et FECN reçus par le routeur. L'état du circuit virtuel permanent peut être actif, inactif ou supprimé.

La commande **show frame-relay pvc** présente l'état de tous les circuits virtuels permanents configurés sur le routeur. Spécifiez un circuit virtuel permanent pour afficher son état en particulier. À la figure 3, la commande **show frame-relay pvc 100** affiche uniquement l'état du circuit virtuel permanent PVC 100.

Utilisez la commande **show frame-relay map** pour afficher les entrées actuelles de la carte, ainsi que des informations sur les connexions. Les informations ci-dessous permettent d'interpréter l'écran de résultats **show frame-relay map** qui apparaît à la figure 4:

```
Router#show frame-relay map
Serial0/0 (up) : ip 10.140.1.1 dlci 100 (0x64,0x1840),
                 dynamic, broadcast, status defined, active
```

- 10.140.1.1 constitue l'adresse IP du routeur distant, apprise de façon dynamique par la résolution d'adresse inverse
- 100 est la valeur décimale de l'identificateur DLCI local
- 0x64 est la conversion hexadécimale de l'identificateur DLCI, 0x64 = 100 en valeur décimale
- 0x1840 est la valeur telle qu'elle apparaît sur la ligne, étant donné que les bits de l'identificateur DLCI sont dispersés dans le champ d'adresse de la trame Frame Relay
- La diffusion broadcast/multicast est activée sur le circuit virtuel permanent
- L'état du circuit virtuel permanent est actif

Pour supprimer les cartes Frame Relay créées de façon dynamique à l'aide de la résolution d'adresse inverse, utilisez la commande **clear frame-relay-inarp**. 5

```
Router#show frame-relay map
Serial0/0 (up): ip 10.40.1.1 dlci 100 (0x64,0x1840),
                dynamic, broadcast, status defined, active
Router#clear frame-relay inarp
Router#show frame-relay map
Router#
```

Activité de TP

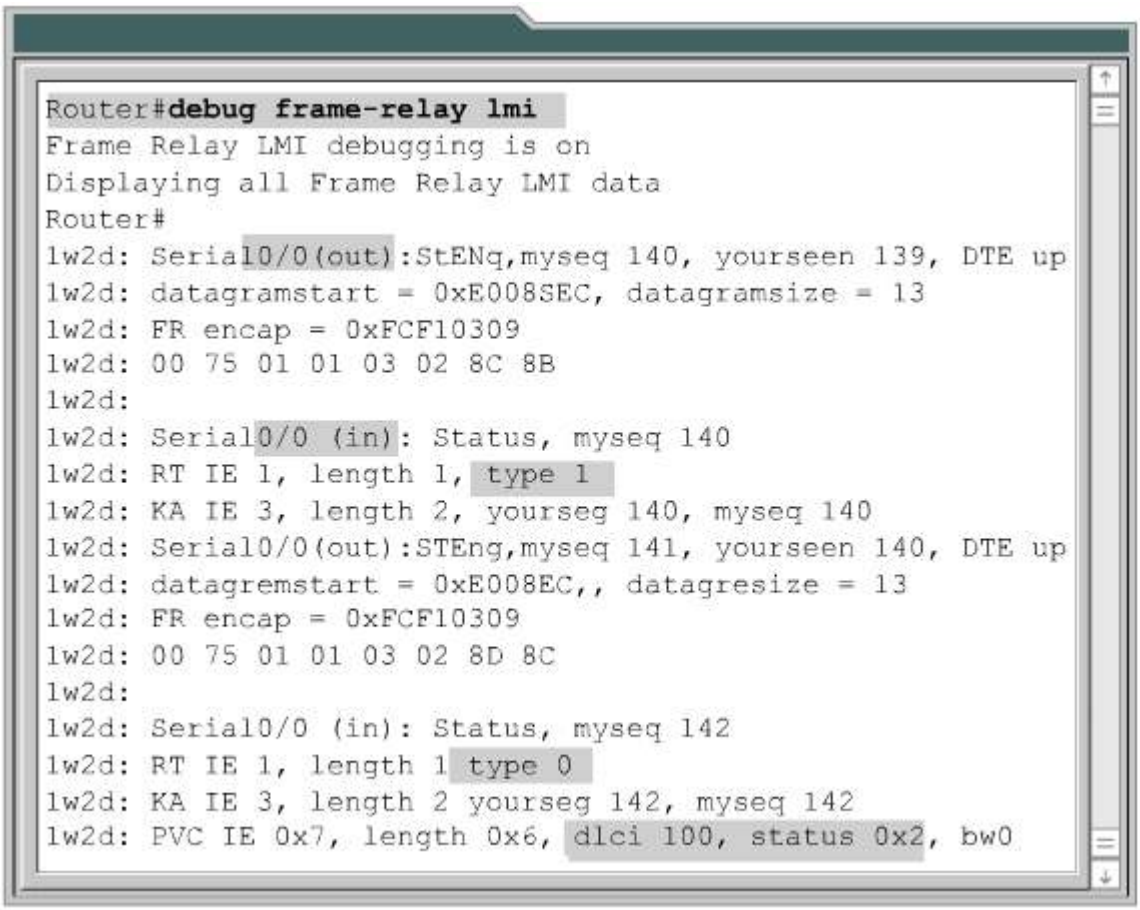
Activité en ligne: show frame-relay pvc

Au cours de cette activité, l'étudiant va apprendre l'utilisation de la commande **`show frame-relay pvc`** pour afficher des statistiques sur les circuits virtuels permanents des interfaces Frame Relay.

5.2 Configuration de Frame Relay

5.2.7 Dépannage de la configuration Frame Relay

Utilisez la commande **`debug frame-relay lmi`** pour déterminer si le routeur et le commutateur Frame Relay envoient et reçoivent correctement les paquets LMI. 1



```
Router#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Router#
1w2d: Serial0/0(out):StENq,myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008SEC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0/0 (in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0/0(out):STEng,myseq 141, yourseen 140, DTE up
1w2d: datagremstart = 0xE008EC,, datagresize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0/0 (in): Status, myseq 142
1w2d: RT IE 1, length 1 type 0
1w2d: KA IE 3, length 2 yourseq 142, myseq 142
1w2d: PVC IE 0x7, length 0x6, dlci 100, status 0x2, bw0
```

Le «out» est un message d'état de l'interface LMI envoyé par le routeur. Le «in» est un message reçu du commutateur Frame Relay. Un message d'état LMI complet est un «type 0». Un échange LMI est un «type 1». «dlci 100, status 0x2» indique l'état actif de l'identificateur DLCI 100. Les valeurs possibles du champ d'état sont les suivantes :

- **0x0** – Ajouté/inactif signifie qu'un identificateur DLCI a été programmé pour le commutateur, mais qu'il n'est pas utilisable. La raison peut en être que l'autre extrémité du circuit virtuel permanent ne fonctionne pas.
- **0x2** – Ajouté/actif signifie que le commutateur Frame Relay dispose de l'identificateur DLCI et que tout est opérationnel.
- **0x4** – Supprimé signifie que le commutateur Frame Relay n'a programmé aucun identificateur DLCI pour le routeur, mais qu'il en a existé un dans le passé. Ceci est peut-être causé par l'inversion des DLCI sur le routeur ou parce que le circuit virtuel permanent a été supprimé par l'opérateur dans le nuage Frame Relay.

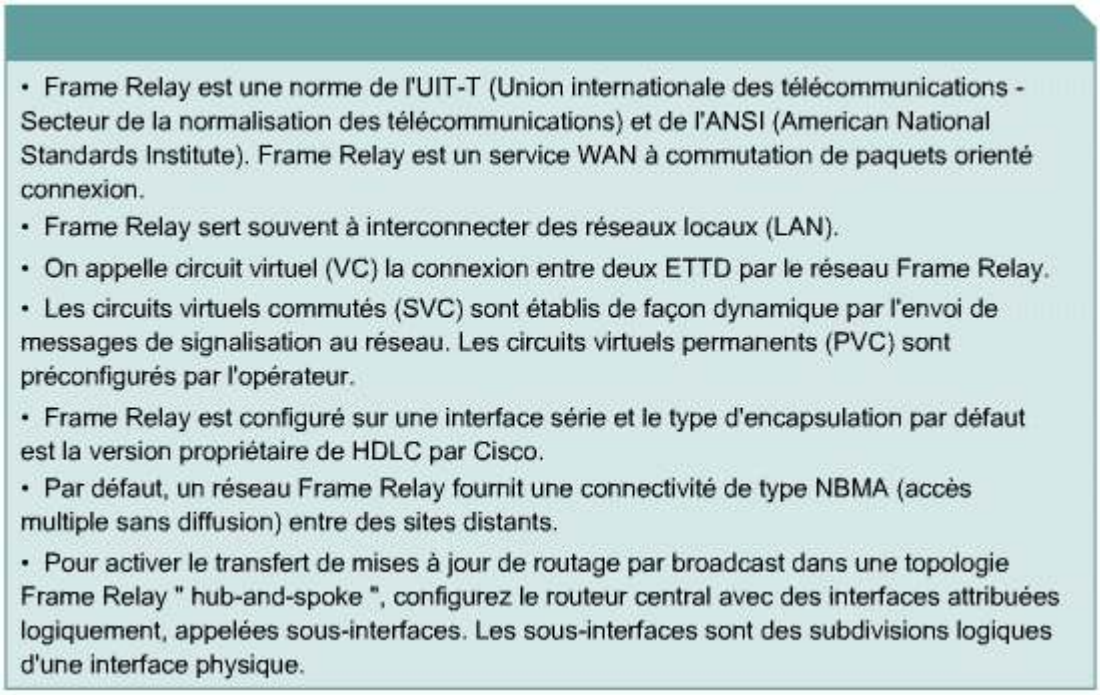
Activité de TP

Activité en ligne: Configuration de Frame Relay. Au cours de cette activité, l'étudiant va effectuer des configurations de base de Frame Relay.

Résumé

La compréhension des points clés suivants devrait être acquise:

- La portée et la fonction de Frame Relay
- La technologie de Frame Relay
- Les topologies point-à-point et point-à-multipoint
- La topologie d'un réseau Frame Relay
- La configuration d'un circuit virtuel permanent (PVC) Frame Relay
- La création d'une carte Frame Relay sur un réseau distant
- Les problèmes potentiels de routage sur un réseau à accès multiple sans diffusion
- La raison pour laquelle des sous-interfaces sont nécessaires et leur mode de configuration
- La vérification et le dépannage d'une connexion Frame Relay


• Frame Relay est une norme de l'UIT-T (Union internationale des télécommunications - Secteur de la normalisation des télécommunications) et de l'ANSI (American National Standards Institute). Frame Relay est un service WAN à commutation de paquets orienté connexion.
• Frame Relay sert souvent à interconnecter des réseaux locaux (LAN).
• On appelle circuit virtuel (VC) la connexion entre deux ETTD par le réseau Frame Relay.
• Les circuits virtuels commutés (SVC) sont établis de façon dynamique par l'envoi de messages de signalisation au réseau. Les circuits virtuels permanents (PVC) sont préconfigurés par l'opérateur.
• Frame Relay est configuré sur une interface série et le type d'encapsulation par défaut est la version propriétaire de HDLC par Cisco.
• Par défaut, un réseau Frame Relay fournit une connectivité de type NBMA (accès multiple sans diffusion) entre des sites distants.
• Pour activer le transfert de mises à jour de routage par broadcast dans une topologie Frame Relay " hub-and-spoke ", configurez le routeur central avec des interfaces attribuées logiquement, appelées sous-interfaces. Les sous-interfaces sont des subdivisions logiques d'une interface physique.

Vue d'ensemble

Les premiers PC ont été conçus comme des systèmes de bureau autonomes. Le système d'exploitation ne permettait qu'à un utilisateur à la fois d'accéder aux fichiers et aux ressources du système. L'utilisateur disposait d'un accès physique au PC. À mesure que les réseaux informatiques de PC gagnaient en popularité dans les entreprises, les éditeurs de logiciels ont commencé à développer des systèmes d'exploitation de réseau spécialisés (NOS). Les développeurs ont conçu les systèmes d'exploitation de réseau pour sécuriser les fichiers, fournir des privilèges utilisateur et partager les ressources entre de nombreux utilisateurs. La croissance explosive d'Internet a mené ces développeurs à créer les systèmes d'exploitation réseau d'aujourd'hui autour des technologies relatives à Internet et des services comme le World Wide Web (WWW).

La connectivité réseau est aujourd'hui un composant essentiel de l'informatique de bureau. La distinction entre les systèmes d'exploitation de bureau modernes, désormais débordant de fonctionnalités et services réseau et leurs homologues de réseau est devenue très vague. Désormais, les systèmes d'exploitation les plus répandus, tels que Microsoft Windows 2000 et Linux peuvent aussi bien être trouvés sur des serveurs réseau surpuissants que sur les postes des utilisateurs de base.

La connaissance des différents systèmes d'exploitation assure que c'est le système d'exploitation offrant tous les services nécessaires qui sera sélectionné. UNIX, Linux, Mac OS X et plusieurs systèmes d'exploitation Windows sont présentés dans le présent document.

Une administration efficace des réseaux locaux (LAN) et longue distance (WAN) constitue la clé pour conserver un environnement productif dans le monde des réseaux. Comme un nombre croissant de services est mis à la disposition de plus en plus d'utilisateurs, les performances du réseau en subissent les conséquences. Par une surveillance constante, les administrateurs réseau doivent reconnaître et pouvoir rectifier les problèmes avant même que les utilisateurs de base ne les remarquent.

Divers outils et protocoles permettent de surveiller le réseau localement et à distance. Il est vital de comprendre ces outils en profondeur pour administrer un réseau de façon efficace.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Identifier plusieurs tâches potentielles effectuées par une station de travail
- Identifier plusieurs fonctions potentielles d'un serveur
- Décrire les rôles de l'équipement dans un environnement client/serveur
- Décrire les différences entre un système d'exploitation réseau et de bureau
- Énumérer plusieurs systèmes d'exploitation Windows et leurs fonctionnalités
- Énumérer plusieurs alternatives aux systèmes d'exploitation Windows, avec leurs fonctionnalités
- Identifier les outils d'administration réseau
- Identifier les forces qui régissent l'administration réseau
- Décrire les modèles OSI et d'administration réseau
- Décrire le protocole SNMP (*Simple Network Management Protocol*) et le protocole CMIP (*Common Management Information Protocol*)
- Décrire la manière dont les logiciels d'administration recueillent des informations et consignent les problèmes

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
6.1	Stations de travail et serveurs
6.2	Administration réseau

6.1 Stations de travail et serveurs

6.1.1 Stations de travail

Une station de travail est un ordinateur client utilisé pour exécuter des applications. Elle est connectée à un serveur sur lequel elle obtient des données partagées avec d'autres utilisateurs. Un serveur est un ordinateur qui utilise un système d'exploitation de réseau. Une station de travail utilise des logiciels spéciaux, par exemple un shell de réseau, pour effectuer les activités suivantes:

- Intercepter les données utilisateurs et les commandes des applications
- Décider si la commande est destinée au système d'exploitation local ou au système d'exploitation de réseau
- Diriger la commande vers le système d'exploitation local ou vers la carte réseau (NIC) pour traitement et transmission sur le réseau
- Acheminer les transmissions du réseau vers l'application exécutée sur la station de travail

Certains systèmes d'exploitation Windows peuvent être installés sur des stations de travail et des serveurs. Les versions NT/2000/XP de Windows offrent des fonctionnalités de serveur réseau. Windows versions 9x et ME ne gère que les stations de travail. 1

UNIX ou Linux peuvent servir de systèmes d'exploitation de bureau, mais on les trouve généralement sur les ordinateurs haut de gamme. Ces stations de travail sont utilisées sur des applications techniques et scientifiques, qui nécessitent des ordinateurs hautes performances dédiés. Parmi les applications fréquemment utilisées sur les stations de travail UNIX, on trouve les suivantes:

- Conception assistée par ordinateur (CAO)
- Conception de circuits électroniques
- Analyse de données météorologiques
- Images de synthèse
- Gestion d'équipements de télécommunications

La plupart des systèmes d'exploitation de bureau offrent des fonctions réseau et acceptent les accès multi-utilisateurs. C'est pourquoi il devient plus courant de classer les ordinateurs et les systèmes d'exploitation en fonction des types d'applications qu'ils utilisent. Ce classement se fonde sur le rôle ou la fonction qu'occupe l'ordinateur, à savoir station de travail ou serveur. Parmi les applications typiques pour ordinateurs de bureau et stations de travail bas de gamme, on trouve les traitements de texte, les tableurs et les logiciels de gestion financière. Sur les stations de travail haut de gamme, les applications peuvent être la conception graphique, la gestion d'équipements ou d'autres encore, énumérées plus haut.

Les stations de travail sans disque dur local constituent une catégorie spéciale d'ordinateurs, conçus pour fonctionner en réseau. Comme leur nom l'implique, elles n'ont pas de disques durs, mais possèdent un moniteur, un clavier, de la mémoire, des

instructions de démarrage en ROM, ainsi qu'une carte réseau. Le logiciel servant à établir une connexion réseau se charge à partir de la ROM amorçable située sur la carte réseau.

Comme elles n'ont pas de disque dur, il n'est pas possible de télécharger de données vers et depuis ces stations de travail. Une station de travail sans disque dur local ne peut pas transmettre de virus au réseau, ni servir à prendre des données sur le réseau en les copiant sur un disque dur. Conséquemment, les stations sans disque offrent plus de sécurité que les stations de travail ordinaires. C'est pour cette raison que les stations de travail de ce type sont utilisées sur les réseaux où la sécurité est primordiale.

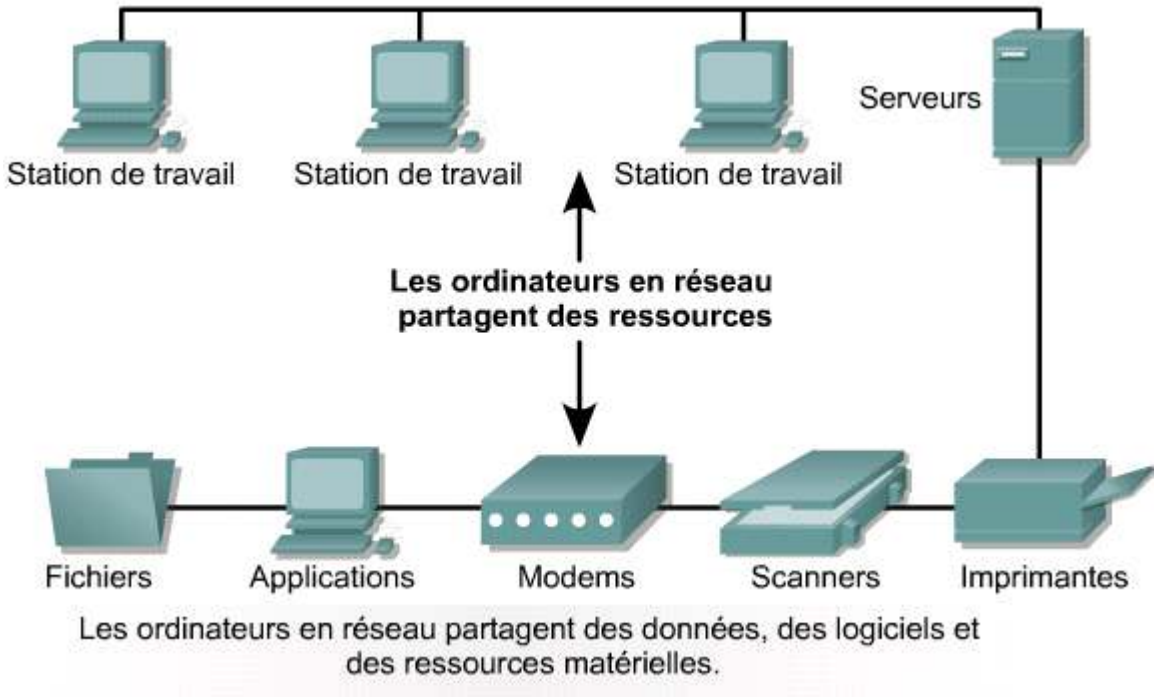
Il est également possible d'utiliser des ordinateurs portables comme stations de travail d'un réseau local en les connectant par une station d'accueil, un adaptateur réseau externe ou une carte PCMCIA. Une station d'accueil est un dispositif d'extension qui transforme un portable en ordinateur de bureau. 3

6.1 Stations de travail et serveurs

6.1.2 Serveurs

Dans un environnement de système d'exploitation de réseau, de nombreux systèmes clients accèdent à un ou plusieurs serveurs pour en partager les ressources. 1

Les systèmes clients de bureau sont équipés de mémoire et de périphériques, tels qu'un clavier, un moniteur et un disque dur. Les systèmes serveurs doivent être équipés pour prendre en charge de nombreux utilisateurs simultanés et de nombreuses tâches à mesure que les clients exigent du serveur des ressources à distance. 2

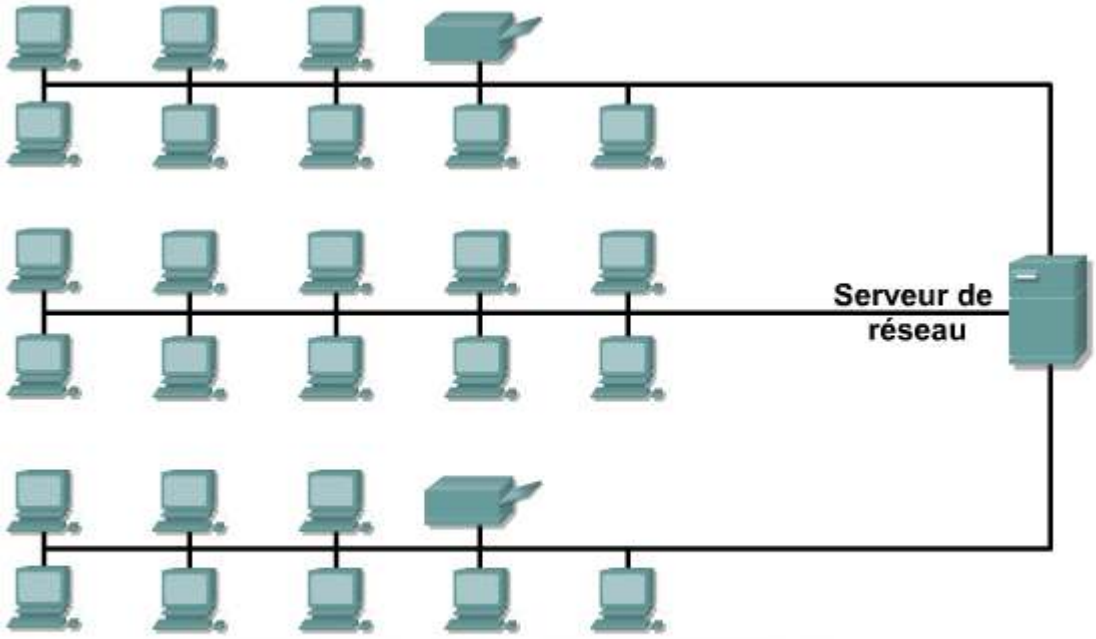


Les systèmes d'exploitation de réseau comportent d'autres outils et fonctions d'administration réseau conçus pour gérer les accès par de grands nombres d'utilisateurs simultanés. Sur tous les réseaux à l'exception des plus petits, les systèmes d'exploitation de réseau sont installés sur des serveurs haut de gamme. De nombreux utilisateurs, les clients, partagent ces serveurs. Les serveurs disposent généralement de disques durs haute capacité et rapides, de grandes quantités de mémoire vive, de cartes réseau rapides et, dans certains cas, de plusieurs processeurs. Ces serveurs sont généralement configurés pour exploiter la famille de protocoles d'Internet, TCP/IP, et pour offrir un ou plusieurs services TCP/IP.

Les serveurs équipés de systèmes d'exploitation de réseau servent également à authentifier les utilisateurs et à accéder à des ressources partagées. Ces serveurs sont conçus pour gérer simultanément les requêtes de nombreux clients. Avant qu'un client ne puisse accéder aux ressources du serveur, il doit être identifié, puis autorisé à utiliser ces ressources. L'identification et l'autorisation s'obtiennent en attribuant à chaque client un nom de compte et un mot de passe. Ce nom et ce mot de passe sont ensuite vérifiés par un service d'authentification qui autorise ou refuse l'accès au réseau. En centralisant les comptes utilisateurs, la sécurité et le contrôle d'accès, les réseaux client/serveur simplifient l'administration réseau.

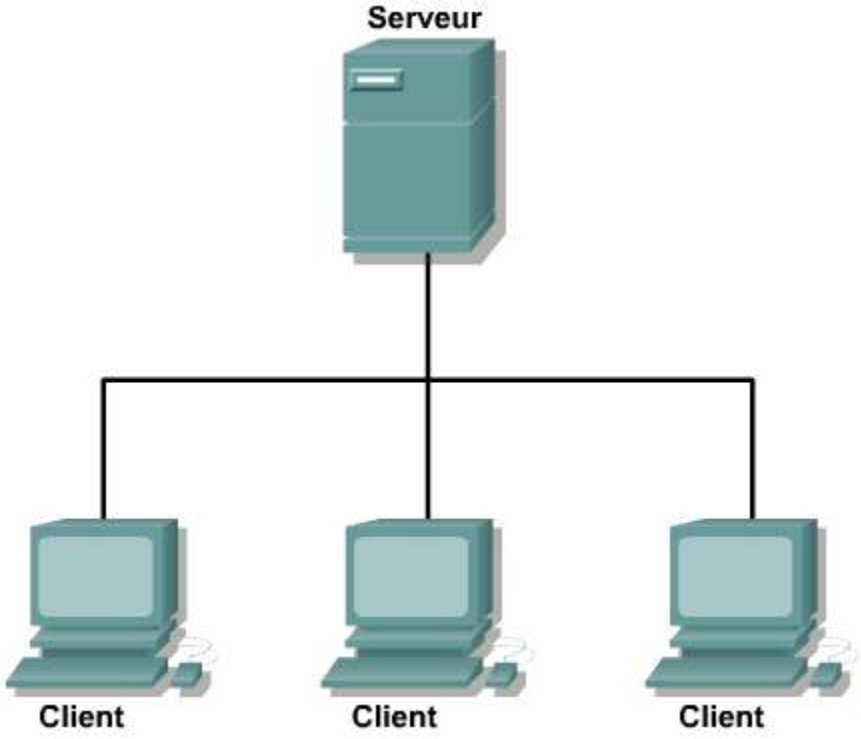
Les serveurs sont généralement de plus grande capacité que les stations de travail et disposent de mémoire supplémentaire pour traiter simultanément les nombreuses tâches actives ou résidant en mémoire. Les serveurs ont également besoin d'espace disque supplémentaire pour stocker les fichiers partagés et pour servir d'extension à la mémoire interne du système. Les cartes système des serveurs nécessitent des connecteurs d'extension supplémentaires pour y connecter des périphériques partagés, tels que des imprimantes et plusieurs interfaces réseau.

La puissance de traitement est une autre caractéristique des systèmes pouvant être utilisés comme serveurs. Habituellement, les ordinateurs sont dotés d'un processeur unique exécutant les instructions qui constituent une tâche ou un processus. Pour fonctionner efficacement et fournir des réponses rapides aux requêtes des clients, un serveur géré par système d'exploitation de réseau nécessite un processeur efficient pour exécuter ses tâches ou ses programmes. Les systèmes monoprocesseur peuvent répondre aux besoins de la plupart des serveurs si ce processeur fournit la vitesse nécessaire. Pour obtenir des vitesses d'exécution plus élevées, certains systèmes sont équipés de plusieurs processeurs. On les appelle systèmes multiprocesseurs. Ces systèmes sont capables d'exécuter plusieurs tâches en parallèle en attribuant chacune d'entre elles à un processeur distinct. La quantité agrégée de travail que le serveur peut exécuter en un temps donné est largement augmentée sur un système multiprocesseur. 3

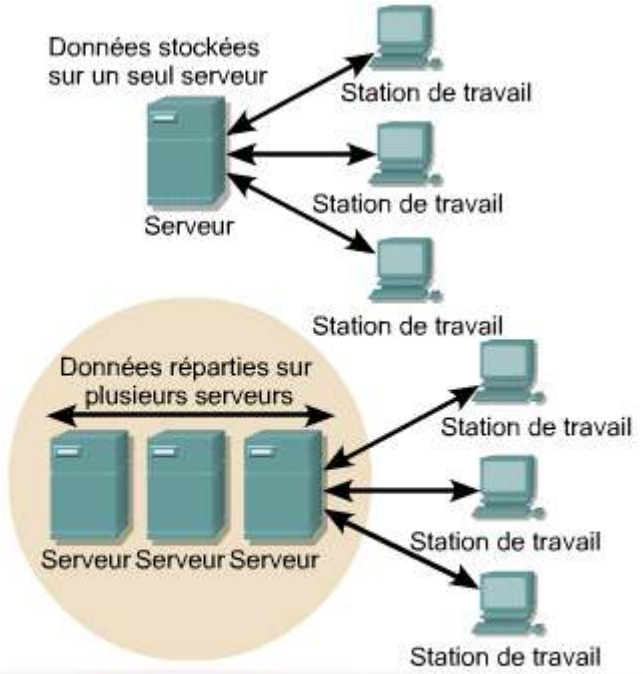


Un serveur de réseau peut gérer plusieurs utilisateurs et équipements.

Comme les serveurs fonctionnent comme des référentiels centraux de ressources vitales au fonctionnement des systèmes clients, ces serveurs doivent être efficaces et robustes. Le terme robuste indique que les systèmes serveurs sont capables de fonctionner efficacement sous de lourdes charges. Il signifie également que les systèmes peuvent survivre à la défaillance d'un ou plusieurs processus ou composants sans qu'une défaillance générale du système se produise. Pour atteindre cet objectif, des fonctions de redondance sont intégrées aux systèmes serveurs. La redondance désigne l'inclusion de composants matériels supplémentaires pouvant prendre la priorité en cas de défaillance d'autres composants. La redondance est une fonction des systèmes à tolérance d'erreurs conçus pour survivre aux pannes et pouvant être réparés sans interruption de leur activité. Comme un système d'exploitation de réseau dépend de l'activité ininterrompue de son serveur, les composants matériels supplémentaires justifient les dépenses supplémentaires. 4

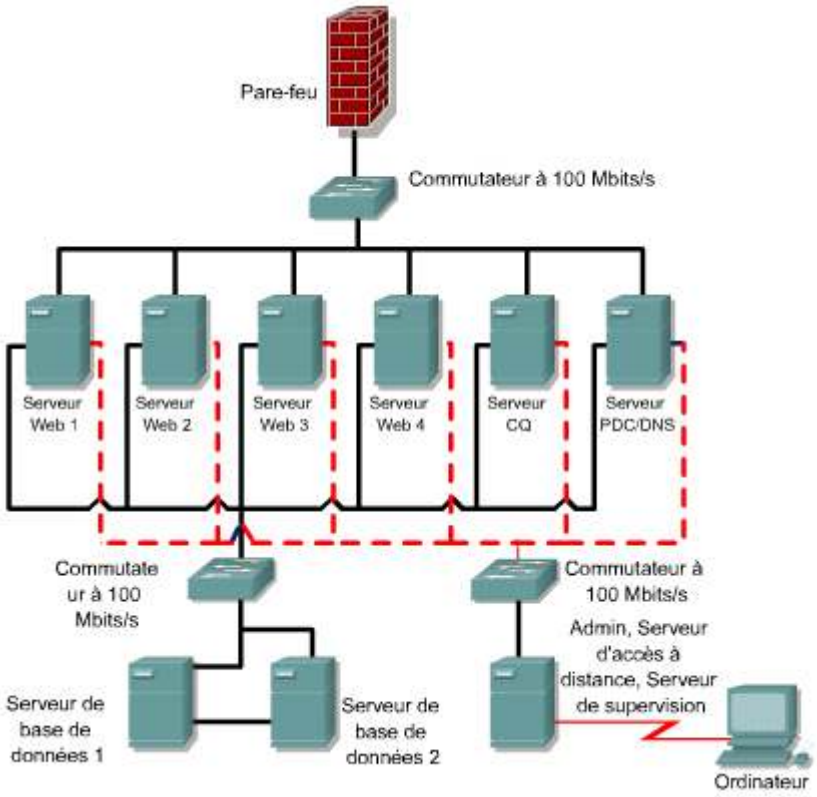


Les applications et fonctions du serveur incluent notamment les services Web utilisant le protocole HTTP (*Hypertext Transfer Protocol*), le protocole FTP (*File Transfer Protocol*) et DNS (Système de noms de domaine). Les protocoles de courrier électronique standard pris en charge par les serveurs réseau incluent SMTP (*Simple Mail Transfer Protocol*), POP3 (*Post Office Protocol 3*) et IMAP (*Internet Messaging Access Protocol*). Les protocoles de partage de fichiers incluent NFS (*Sun Microsystems Network File System*) et SMB (*Microsoft Server Message Block*). 5



Les données peuvent résider sur un seul serveur ou être réparties sur plusieurs serveurs.

Les serveurs réseau fournissent fréquemment des services d'impression. Un serveur peut également offrir le protocole DHCP (*Dynamic Host Configuration Protocol*), qui alloue automatiquement des adresses IP à des stations de travail clientes. Outre l'exécution de services pour les clients du réseau, les serveurs peuvent également servir de pare-feu de base pour le réseau. Pour ce faire, on utilise un proxy ou la fonction de traduction d'adresses réseau NAT (*Network Address Translation*), qui masquent tous deux les adresses réseau privées pour Internet. 6



Un serveur équipé d'un système d'exploitation de réseau peut fonctionner correctement en ne desservant qu'une poignée de clients. Toutefois, la plupart des entreprises déploient plusieurs serveurs afin d'obtenir des performances acceptables. Dans une conception typique, les services sont séparés, de telle sorte qu'un serveur est responsable du courrier électronique, un autre du partage de fichiers, un autre encore des transferts FTP.

La concentration de ressources réseau, telles que fichiers, imprimantes et applications sur des serveurs rend également les données générées plus faciles à sauvegarder et à gérer. Au lieu d'être réparties sur des machines individuelles, les ressources réseau peuvent résider sur des serveurs spécialisés dédiés, afin d'en faciliter l'accès et la sauvegarde.

Activité de média interactive

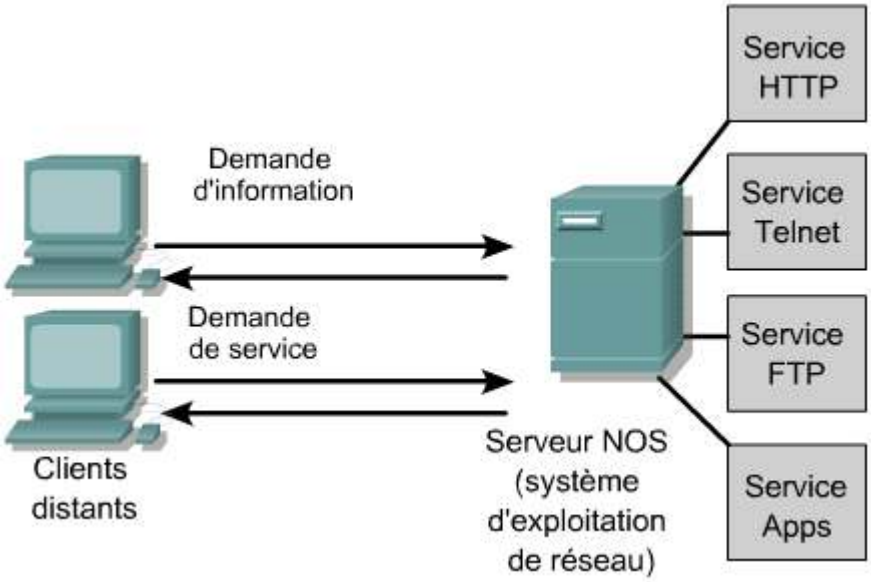
Agrandissement: Composants du serveur

Dans cette vue agrandie, l'étudiant peut observer les composants d'un serveur.

6.1 Stations de travail et serveurs

6.1.3 Relation client-serveur

Le modèle d'architecture client-serveur distribue le traitement sur plusieurs ordinateurs. Le traitement distribué permet d'accéder à des systèmes distants dans l'objectif de partager des informations et des ressources réseau. Dans un environnement client-serveur, le client et le serveur partagent ou distribuent la responsabilité du traitement. La plupart des systèmes d'exploitation de réseau sont conçus sur le modèle client-serveur afin de fournir des services de réseau aux utilisateurs. Un ordinateur d'un réseau peut être désigné par les termes hôte, station de travail, client ou serveur. Un ordinateur qui utilise TCP/IP, qu'il s'agisse d'une station de travail ou d'un serveur, est considéré comme un ordinateur hôte. 1



Les autres termes couramment utilisés sont:

- **Hôte local** – Machine sur laquelle l'utilisateur travaille habituellement.
- **Hôte distant** – Système auquel un utilisateur accède à partir d'un autre système.
- **Serveur** – Fournit des ressources à un ou plusieurs clients par le biais d'un réseau.
- **Client** – Machine utilisant les services d'un ou plusieurs serveurs réseau.

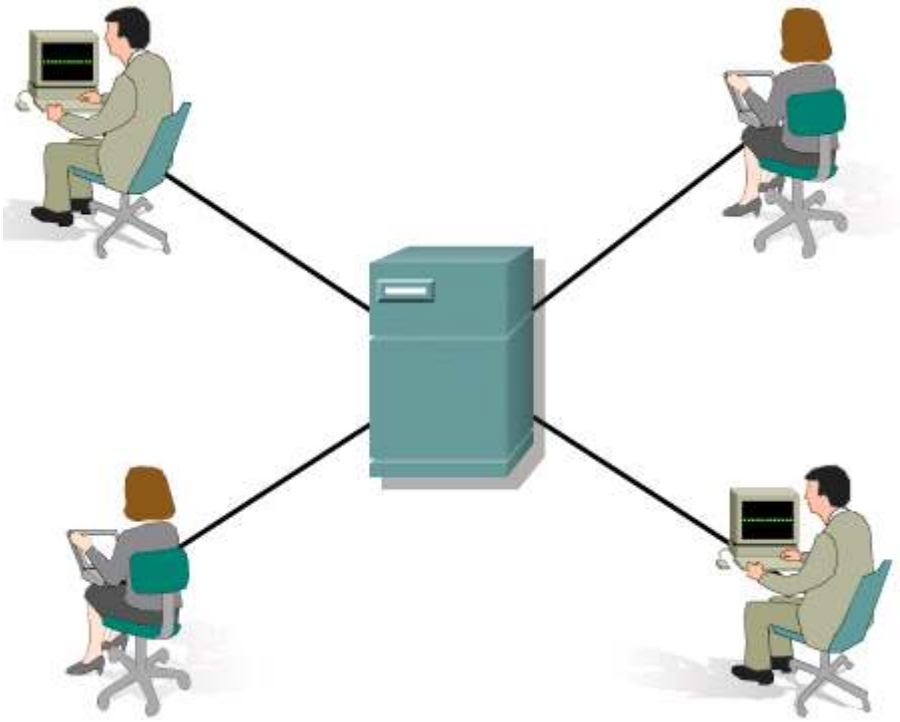
Une session FTP constitue un exemple de relation client-serveur. FTP est une méthode universelle de transfert d'un fichier d'un ordinateur à l'autre. Pour que le client puisse transférer un fichier vers ou depuis le serveur, ce dernier doit comporter un démon ou un service FTP. Dans ce cas, le client demande le transfert du fichier. Le serveur fournit les services nécessaires à la réception ou à l'envoi du fichier.

Internet constitue également un bon exemple de relation client-serveur par traitement distribué. Le client, ou ordinateur frontal, gère généralement les fonctions de présentation utilisateur, telles que le format d'écran, les formulaires de saisie et l'édition de données. Pour ce faire, on utilise un navigateur, tel que Netscape ou Internet Explorer. Les navigateurs Web envoient des requêtes à des serveurs Web. Quand le navigateur demande des données au serveur, celui-ci répond et le programme reçoit la réponse. Le navigateur affiche ensuite les données HTTP qu'il a reçues. Le serveur, ou back end, gère les demandes de pages Web du client et fournit des services HTTP ou WWW.

Un serveur de base de données et un client de saisie de données ou d'interrogation sur un réseau local constituent un autre exemple de relation client-serveur. Le client, ou frontal, peut exécuter une application écrite en langage C ou Java et le serveur, ou

back end, peut exécuter Oracle ou un autre logiciel de gestion de bases de données. Dans ce cas, le client gère les tâches de mise en forme et de présentation pour l'utilisateur. Le serveur fournit des services de stockage de la base de données et de récupération des données pour l'utilisateur.

Dans un environnement typique de serveur de fichiers, le client peut être amené à récupérer des parties importantes des fichiers de la base de données afin d'effectuer un traitement local. Cette récupération de fichiers de la base de données peut occasionner un trafic réseau excessif. Avec le modèle client-serveur, le client présente une requête au serveur et le moteur de base de données du serveur peut traiter 100 000 enregistrements pour n'en renvoyer que quelques-uns au client en vue de satisfaire la requête. Les serveurs sont généralement bien plus efficaces que les ordinateurs clients, ainsi que mieux adaptés au traitement de grandes quantités de données. Avec l'architecture client-serveur, la base de données de grande taille est stockée et le traitement s'effectue sur le serveur. La seule tâche du client consiste à créer la requête. Une quantité relativement réduite de données ou de résultats peut être transmise par le réseau. Ceci satisfait la requête du client et permet de moins utiliser la bande passante du réseau. Le graphique montre un exemple d'architecture client-serveur. Notez que la station de travail et le serveur sont normalement connectés au réseau local par un concentrateur ou un commutateur. 2



La distribution des fonctions dans un réseau client-serveur offre des avantages substantiels, mais implique également des coûts. Bien que l'agrégation des ressources sur les systèmes serveurs offre plus de sécurité, un accès simplifié et un contrôle coordonné, le serveur constitue l'unique point de défaillance du réseau. En effet, sans un serveur opérationnel, le réseau ne peut plus fonctionner. Par ailleurs, un personnel expert formé est nécessaire pour l'administration et la maintenance des serveurs, ce qui augmente encore le coût d'exploitation du réseau. Les systèmes serveurs nécessitent du matériel complémentaire et des logiciels spécialisés qui en augmentent le coût de façon significative.

6.1 Stations de travail et serveurs

6.1.4 Introduction aux systèmes d'exploitation de réseau

Le système d'exploitation d'un ordinateur constitue la fondation logicielle sur laquelle les applications et les services s'exécutent. De même, un système d'exploitation de réseau autorise la communication entre plusieurs équipements et le partage de ressources sur l'ensemble d'un réseau. Un système d'exploitation réseau peut fonctionner sur des serveurs UNIX, ou Microsoft Windows. 1

Novell	UNIX	Windows	Linux
NetWare	HP-UX	NT	Red Hat
IntraNetWare	Sun Solaris	Server 2000	Caldera
GroupWise	BSD	.NET Server	SuSE
	SCO	Server 2003	Debian
	AIX		Slackware

Les fonctions courantes du système d'exploitation d'une station de travail sont notamment le contrôle du matériel, l'exécution de programmes et la mise à disposition d'une interface utilisateur. Le système d'exploitation exécute ces fonctions pour un seul utilisateur. Plusieurs utilisateurs peuvent partager la machine, mais ne peuvent pas se connecter en même temps. En contraste, un système d'exploitation de réseau distribue des fonctions sur un certain nombre d'ordinateurs en réseau. Un système d'exploitation de réseau dépend du système d'exploitation natif de chaque ordinateur individuel. Le système d'exploitation de réseau ajoute ensuite des fonctionnalités autorisant l'accès simultané de plusieurs utilisateurs aux ressources partagées.

Les stations de travail servent de clients dans ce type d'environnement. Quand une station devient client dans un environnement de système d'exploitation de réseau, des logiciels spécialisés complémentaires permettent à l'utilisateur local d'accéder à des ressources non locales ou distantes comme si celles-ci faisaient partie de son système local. Le système d'exploitation de réseau améliore la portée de la station de travail cliente en mettant à disposition les services distants en tant qu'extensions du système d'exploitation local.

Un système capable de fonctionner comme un serveur de système d'exploitation de réseau doit pouvoir prendre en charge plusieurs utilisateurs simultanés. L'administrateur réseau crée un compte pour chaque utilisateur, afin de permettre à cet utilisateur d'ouvrir une session et de se connecter au système serveur. Le compte utilisateur sur le serveur permet à ce dernier d'authentifier l'utilisateur et de lui allouer les ressources auxquelles il est autorisé à accéder. Les systèmes qui offrent ces fonctions sont appelés des systèmes multi-utilisateurs.

Un serveur avec système d'exploitation de réseau est un système multitâche, capable d'exécuter plusieurs tâches ou processus en même temps. Le logiciel de planification du système d'exploitation de réseau alloue du temps processeur, de la mémoire et d'autres éléments du système à différentes tâches, de manière à leur permettre de partager les ressources du système. Chaque utilisateur d'un système multi-utilisateur est pris en charge en interne par une tâche ou un processus du serveur. Ces tâches internes sont créées de façon dynamique à mesure que les utilisateurs se connectent au système et sont supprimées lorsqu'ils se déconnectent.

Les principales caractéristiques à prendre en compte pour la sélection d'un système d'exploitation de réseau sont les performances, les outils d'administration et de surveillance, la sécurité, l'évolutivité et la robustesse ou tolérance d'erreurs. La section ci-dessous fournit une brève description de ces caractéristiques.

Considérations relatives au système d'exploitation de réseau		
Sécurité	Cryptage	Authentification des utilisateurs
Robustesse	Charges de travail symétriques	Redondance
Performances	Constance lorsque la charge augmente	
Évolutivité	Évolutivité	
Gestion	Administration du système	

Performances
Un système d'exploitation de réseau doit offrir de bonnes performances en lecture et en écriture de fichiers sur le réseau entre les clients et les serveurs. Il doit pouvoir maintenir des performances rapides sous de lourdes charges, quand de nombreux clients émettent des requêtes. Des performances homogènes sous de lourdes charges représentent une norme importante pour un système d'exploitation de réseau.

Administration et surveillance
L'interface de gestion du serveur équipé d'un système d'exploitation de réseau fournit les outils de surveillance du serveur, l'administration des clients et de gestion des fichiers, de l'impression et du stockage. L'interface d'administration fournit les outils nécessaires à l'installation de nouveaux services et à la configuration de ces services. De plus, les serveurs demandent une surveillance et des réglages réguliers.

Sécurité
Un système d'exploitation de réseau doit protéger les ressources partagées qu'il contrôle. La sécurité inclut l'authentification des accès utilisateurs aux services, afin d'empêcher les accès non autorisés aux ressources du réseau. La sécurité sert également à crypter les informations pour les protéger pendant qu'elles sont acheminées entre les clients et les serveurs.

Évolutivité
L'évolutivité indique la capacité de croissance sans dégradation des performances d'un système d'exploitation de réseau. Le système d'exploitation doit pouvoir maintenir ses performances à mesure que de nouveaux utilisateurs se joignent au réseau et que de nouveaux serveurs y sont ajoutés pour les prendre en charge.

Robustesse/tolérance d'erreurs

La robustesse indique la capacité à fournir des services de façon homogène sous de lourdes charges, et à maintenir ses services en cas de défaillance de composants ou de processus. L'utilisation de disques durs redondants et l'équilibrage de la charge sur plusieurs serveurs peuvent améliorer la robustesse d'un système d'exploitation de réseau.

6.1 Stations de travail et serveurs

6.1.5 Microsoft NT, 2000 et .NET

Depuis la sortie de Windows 1.0 en novembre 1985, Microsoft a produit de nombreuses versions des systèmes d'exploitation Windows, avec des améliorations et des modifications destinées à gérer une grande diversité d'utilisateurs et de fonctions. La figure 1 résume le système d'exploitation Windows actuel.

Système d'exploitation	Versions	Utilisations
Windows NT	• Workstation • Server	• Utilisateurs en entreprise • Serveur départemental
Windows 2000	• Professional • Server • Advanced server • .NET	• Utilisateurs en entreprise ou petites entreprises • Serveur d'accès à distance ou Internet • Serveur départemental • Serveur d'entreprise • Serveur Internet d'entreprise

NT 4 a été conçu pour les opérations d'une importance capitale, dans le but de fournir un environnement plus stable que les systèmes d'exploitation grand public de Microsoft. Il est disponible dans des versions de bureau (NT 4.0 Workstation) et serveur (NT 4.0 Server). Par rapport aux systèmes d'exploitation Microsoft précédents, NT offre l'avantage de pouvoir exécuter DOS et des programmes Windows plus anciens dans des machines virtuelles (VM). Les défaillances du programme sont isolées et ne demandent aucun redémarrage du système.

Windows NT fournit une structure de domaine permettant de contrôler l'accès des utilisateurs et des clients aux ressources du serveur. Elle est administrée par l'application User Manager for Domains sur le contrôleur de domaine. Chaque domaine NT nécessite un seul contrôleur de domaine primaire, qui contient la base de données SAM (*Security Accounts Management Database*) et peut disposer d'un ou plusieurs contrôleurs de domaine de secours, chacun d'entre eux contenant une copie en lecture seule de la base SAM. Quand un utilisateur tente de se connecter, les informations de son compte sont envoyées à la base de données SAM. Si les informations liées à ce compte sont stockées dans la base de données, l'utilisateur est authentifié vis-à-vis du domaine et peut accéder aux ressources de la station de travail et du réseau.

S'appuyant sur le noyau NT, la version 2000 de Windows, plus récente, existe également dans des versions de bureau et serveur. Windows 2000 prend en charge la technologie «plug-and-play», qui permet d'installer de nouveaux équipements sans qu'il soit nécessaire de redémarrer le système. Windows 2000 inclut également un système de cryptage de fichiers afin de sécuriser les données du disque dur.

Windows 2000 permet de placer des objets, tels que des utilisateurs et des ressources, dans des objets conteneurs appelés unités organisationnelles (OU). L'autorité d'administration de chaque OU peut être déléguée à un utilisateur ou à un groupe. Cette fonction permet de procéder à un contrôle plus spécifique qu'avec Windows NT 4.0.

Windows 2000 Professional n'est pas conçu pour être un système d'exploitation de réseau complet. Il ne fournit ni contrôleur de domaine, ni serveur DNS, ni serveur DHCP, et ne rend aucun des services pouvant être déployés avec Windows 2000 Server. La fonction principale de Windows 2000 Professional est de faire partie d'un domaine dans le rôle de système d'exploitation côté client. Le type de matériel pouvant être installé sur le système est limité. Windows 2000 Professional peut fournir des capacités limitées de serveur pour les petits réseaux et les réseaux d'égal à égal. Il peut être serveur de fichiers, serveur d'impression, serveur FTP et serveur Web, mais n'accepte que jusqu'à dix connexions simultanées.

Windows 2000 Server ajoute de nombreuses fonctions serveur spécifiques aux fonctionnalités de Windows 2000 Professional. Il peut également fonctionner comme serveur de fichiers, d'impression, Web et d'applications. La fonction Active Directory Services de Windows 2000 Server sert de point centralisé pour la gestion des utilisateurs, groupes, services de sécurité et ressources de réseau. Elle inclut les fonctions universelles requises pour les groupes de travail et les filiales, ainsi que pour le déploiement par service de serveurs de fichiers et d'impression, d'applications, Web et de communication.

Windows 2000 Server est destiné aux environnements des petites et moyennes entreprises. Il offre une connectivité intégrée avec les systèmes Novell NetWare, UNIX et AppleTalk. Il peut également être configuré en tant que serveur de communications pour fournir des services de réseau par accès commuté aux utilisateurs mobiles. Windows 2000 Advanced Server offre le matériel et les logiciels complémentaires requis pour les réseaux d'entreprise et de très grande taille.

Windows .NET Server a été élaboré à partir du noyau de Windows 2000 Server, mais sa conception lui permet de fournir un système sécurisé et fiable pour les sites Web et FTP de l'entreprise, dans le but de rivaliser avec les systèmes d'exploitation serveurs Linux, UNIX et Novell One NET. Windows .NET Server fournit des services Web XML aux sociétés dont le trafic Web varie de moyen à élevé.

6.1 Stations de travail et serveurs

Origines d'UNIX

UNIX est le nom d'un groupe de système d'exploitation dont l'origine remonte aux laboratoires Bell de 1969. Depuis sa création, UNIX a été conçu pour prendre en charge les multi-utilisateurs et le multitâche. UNIX a également été l'un des premiers systèmes d'exploitation à prendre en charge les protocoles réseau d'Internet. L'histoire d'UNIX, qui a maintenant plus de 30 ans, est compliquée, car de nombreuses sociétés et entreprises ont contribué à son développement. 1

- 1969 - Ken Thompson et Dennis Ritchie de la société AT&T Bell Laboratories commencent le développement de ce qui allait devenir UNIX.
- 1973 - UNIX est réécrit en langage C. Il devient ainsi un système d'exploitation portable, capable de s'exécuter sur différents ordinateurs.
- 1975 - La version 6 est distribuée en dehors de Bell Labs. La première version BSD (1.x) est dérivée de cette version 6.
- 1980 - Microsoft présente Xenix et 4.2 BSD est utilisé à grande échelle.
- 1982 - Le groupe USG (UNIX System Group) d'AT&T publie System III, la première version publique utilisée à l'extérieur de Bell Labs.
- 1984 - L'université de Berkeley distribue 4.2 BSD, laquelle comprend le protocole TCP/IP. Sortie de System V Release 2 (SVR2). Environ 100 000 installations UNIX.
- 1986 - Sortie de 4.3 BSD, avec serveur de noms Internet.
- 1987 - Sortie de System V Release 3 (SVR3). On compte environ 750 000 installations UNIX dans le monde.
- 1988 - Sortie de UNIX System V Release 4 (SVR4), qui consacre l'union de System V, de BSD et de Xenix.
- 1991 - UNIX System Laboratories (USL) devient une société, dont l'actionnaire majoritaire est AT&T. Linus Torvalds commence le développement de Linux.
- 1992 - USL commercialise UNIX System V Release 4.2 (SVR 4.2). Novell annonce son intention de racheter USL.
- 1993 - Sortie de 4.4 BSD, dernière version de Berkeley. Novell rachète USL.
- 1996 - Naissance de The Open Group, résultat de la fusion de OSF et de X/Open.
- 1999 - UNIX fête ses 30 ans. Sortie du noyau Linux 2.2.
- 2001 - La version 3 de Single UNIX Specification unifie POSIX, The Open Group et divers efforts de l'industrie. Sortie du noyau Linux 2.4.

UNIX a tout d'abord été écrit en langage assembleur, un jeu d'instructions élémentaires qui contrôle les instructions internes d'un ordinateur. Toutefois, UNIX pouvait seulement fonctionner sur un type d'ordinateur spécifique. En 1971, Dennis Ritchie a créé le langage C. En 1973, Ritchie et son collègue programmeur des laboratoires Bell Ken Thompson ont réécrit les programmes du système UNIX en langage C. Le fait que C soit un langage de plus haut niveau a permis de faire migrer UNIX vers d'autres ordinateurs sans trop d'efforts en matière de programmation. La décision de développer ce système d'exploitation transférable s'avéra être la clé du succès d'UNIX. Au cours des années 1970, UNIX évolua grâce au travail de développement des programmeurs de Bell Labs et de plusieurs universités, notamment l'université de Californie à Berkeley. 2 – 3

Fabricant de processeurs	Version du système d'exploitation UNIX	Autres systèmes d'exploitation propriétaires
IBM	AIX, Linux	MVS, VM
Hewlett Packard	HP-UX, Linux	MPE
Digital Equipment Corporation	Tru64, Ultrix, Linux	VMS
Sun Microsystems	Solaris, Linux	
Intel	Solaris, Linux	NetWare, Win9x, NT, Win2000

- Systèmes d'exploitation standard
- Puissant, souple, évolutif et sécurisé
- Pris en charge par plusieurs équipementiers
- Système d'exploitation stable, arrivé à maturité
- Intégration étroite avec les protocoles TCP/IP
- Très répandu pour les applications critiques

Quand UNIX commença à être commercialisé dans les années 1980, il servait à piloter de puissants serveurs réseau, et non des ordinateurs de bureau. Aujourd'hui, il existe des dizaines de versions différentes d'UNIX, dont notamment les suivantes:

- Hewlett Packard UNIX (HP-UX)
- Berkeley Software Design, Inc. (BSD UNIX), qui a produit des dérivés tels que FreeBSD
- Santa Cruz Operation (SCO) UNIX
- Sun Solaris
- IBM UNIX (AIX)

UNIX, sous ses diverses formes, continue à consolider sa position de système d'exploitation fiable et sécurisé destiné aux applications d'importance vitale, indispensables au bon fonctionnement d'une entreprise ou de toute autre organisation. UNIX est également intégré étroitement avec TCP/IP. Initialement, TCP/IP est issu d'UNIX pour répondre aux besoins en matière de communications sur réseaux locaux et longue distance.

L'environnement d'exploitation Solaris de Sun Microsystems et son système d'exploitation central, SunOS, est une mise en oeuvre d'UNIX sur 64 bits, très souple et offrant des performances élevées. Solaris fonctionne sur une grande diversité d'ordinateurs, des PC avec processeur Intel aux gros systèmes et aux super-ordinateurs. Solaris est actuellement la version d'UNIX la plus utilisée dans le monde pour les réseaux de grande taille et les sites Web d'Internet. Sun est également à l'origine de la technologie Java «Write Once, Run Anywhere».

Malgré la popularité de Microsoft Windows sur les réseaux locaux d'entreprise, une grande partie d'Internet est pilotée par des systèmes UNIX très efficients. Bien qu'UNIX soit généralement associé à du matériel coûteux et soit peu convivial, des développements récents, dont la création de Linux, sont en train de changer cette image.

Origines de Linux

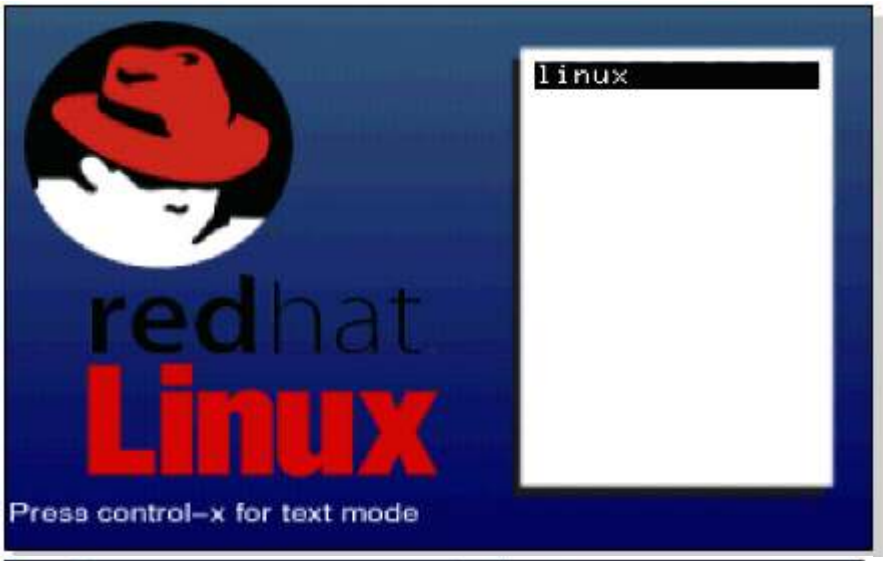
En 1991, un étudiant finlandais du nom de Linus Torvalds commença à travailler sur un système d'exploitation destiné à un ordinateur à processeur Intel 80386. Torvalds fut rapidement frustré par l'état des systèmes d'exploitation de bureau, tels que DOS, et par les coûts et les problèmes de licence associés aux versions commerciales d'UNIX. Torvalds se lança dans le développement d'un système d'exploitation semblable à UNIX dans son fonctionnement, mais utilisa un code logiciel ouvert et totalement gratuit pour tous les utilisateurs.

Le travail de Torvalds mena à un effort de collaboration international pour développer Linux, un système d'exploitation ouvert et semblable à UNIX en termes d'aspect et de confort. À la fin des années 1990, Linux était devenu une alternative viable à UNIX sur les serveurs et à Windows sur les systèmes de bureau. La popularité de Linux sur les PC de bureau a également contribué à l'intérêt vis-à-vis des distributions d'UNIX destinées à ce marché, telles que FreeBSD et Sun Solaris. Les versions de Linux peuvent aujourd'hui fonctionner sur pratiquement n'importe quel processeur 32 bits, dont notamment les puces Intel 80386, Motorola 68000, Alpha et PowerPC.

À l'instar d'UNIX, il existe de nombreuses versions de Linux. Certaines peuvent être téléchargées gratuitement sur le Web et d'autres sont distribuées dans le commerce. Quelques-unes des versions les plus populaires de Linux sont présentées ci-dessous:

- Red Hat Linux – distribué par Red Hat Software
- OpenLinux – distribué par Caldera
- Corel Linux
- Slackware
- Debian GNU/Linux
- SuSE Linux

Aujourd'hui, Linux est l'un des systèmes d'exploitation les plus puissants et les plus fiables du monde. C'est pour cette raison que Linux a commencé à faire son apparition en tant que plate-forme pour les utilisateurs experts et dans le domaine des serveurs d'entreprise. Linux est moins souvent installé en tant que système d'exploitation pour systèmes de bureau d'entreprise. Bien que des interfaces utilisateurs graphiques permettent de rendre Linux plus convivial, la plupart des utilisateurs débutants trouvent qu'il est plus difficile à utiliser que Mac OS ou Windows. Actuellement, de nombreuses sociétés telles que Red Hat, SuSE, Corel et Caldera, s'efforcent de faire de Linux un système d'exploitation viable pour les ordinateurs de bureau. [4] – [7]



Caldera OpenLinux	http://www.caldera.com
Corel Linux	http://linux.corel.com
Debian GNU/Linux	http://www.debian.org
Linux Mandrake	http://linux-mandrake.com/en
Red Hat Linux	http://www.redhat.com
Slackware Linux	http://www.slackware.com
SuSE Linux	http://www.suse.com
Turbo Linux	http://www.turbolinux.com

Il est nécessaire de tenir compte des applications à gérer lorsque l'on met en oeuvre Linux sur un système de bureau. En effet, le nombre d'applications professionnelles de productivité est limité par rapport à ce que l'on peut utiliser avec Windows. Toutefois, certains constructeurs fournissent des logiciels d'émulation Windows, tels que WABI et WINE, qui permettent d'exécuter de nombreuses applications Windows sous Linux. Par ailleurs, des sociétés telles que Corel développent des versions pour Linux de leurs suites bureautiques et d'autres logiciels à succès.

Mise en réseau avec Linux
Les distributions récentes de Linux sont dotées de composants réseau intégrés pour se connecter à un réseau local, établir une connexion commutée vers Internet ou d'autres réseaux distants. En fait, TCP/IP est intégré au noyau Linux au lieu d'être mis en oeuvre comme un sous-système distinct.

Parmi les avantages qu'offre Linux en tant que système d'exploitation de bureau et client de réseau, on peut citer les suivants:

- C'est un véritable système d'exploitation sur 32 bits.
- Il prend en charge le multitâche préemptif et la mémoire virtuelle.
- Son code est ouvert (Open Source) et par conséquent à la disposition de quiconque souhaite l'enrichir ou l'améliorer.

6.1 Stations de travail et serveurs

6.1.7 Apple

Les ordinateurs Apple Macintosh ont été conçus pour une mise en réseau facile dans une situation de groupe de travail d'égal à égal. Les interfaces réseau sont intégrées au matériel, de même que des composants réseau le sont au système d'exploitation Macintosh. Il existe des adaptateurs réseau Ethernet et Token Ring pour le Macintosh.

Le Macintosh, dit Mac, remporte un grand succès dans de nombreuses institutions éducatives et dans les services graphiques des entreprises. Les Mac peuvent être connectés entre eux en groupes de travail et peuvent accéder à des serveurs de fichiers AppleShare. Les Mac peuvent également être connectés à des réseaux locaux de PC contenant des serveurs Microsoft, NetWare ou UNIX. 1

Mac OS X (10)
Le système d'exploitation du Macintosh, Mac OS X, est parfois appelé Apple System 10.

Certaines des fonctions de Mac OS X se trouvent dans l'interface graphique appelée Aqua. L'interface Aqua ressemble à un croisement entre les interfaces graphiques de Microsoft Windows XP et de Linux X-windows. Mac OS X est conçu pour fournir aux ordinateurs familiaux des fonctionnalités telles que la navigation sur Internet, la retouche photo et vidéo et les jeux, tout en fournissant les outils puissants et souples que les professionnels de l'informatique recherchent dans un système d'exploitation. 2

Mac OS X
Mac OSX
version 10.1
Augmentation des performances système globales
Améliorations de l'interface Aqua
Compatibilité réseau exceptionnelle
Lecture et gravure de DVD
Gravure de CD à partir du Finder
Amélioration du graphisme et de l'impression
Mac OS X

Mac OS X est totalement compatible avec des versions plus anciennes des systèmes d'exploitation Mac. Une nouvelle fonction de Mac OS X autorise la connectivité entre AppleTalk et Windows. Le système d'exploitation Mac OS X central est appelé Darwin. Darwin est un système fondé sur UNIX et offrant stabilité et performances élevées. Ces améliorations permettent à Mac OS X de gérer la mémoire protégée, le multitâche préemptif, la gestion avancée de la mémoire et le multitraitement symétrique. Ceci fait de Mac OS X un redoutable concurrent face aux autres systèmes d'exploitation.

6.1 Stations de travail et serveurs

6.1.8 Concept de service sur les serveurs

Les systèmes d'exploitation de réseau sont conçus pour fournir des processus de réseau aux clients. Les services de réseau incluent le WWW, le partage de fichiers, l'échange de courrier électronique, les services d'annuaire, l'administration à distance et les services d'impression. L'administration à distance est un service efficace qui permet aux administrateurs de configurer des systèmes en réseau distants de plusieurs kilomètres. Il est important de comprendre que tous ces processus réseau sont appelés des services sous Windows 2000 et des démons sous UNIX et Linux. Les processus réseau fournissent tous les mêmes fonctions, mais

le chargement et l'interaction de ces processus avec le système d'exploitation de réseau diffèrent avec chaque système d'exploitation. [1] [2] [3]

- Services Web (HTTP)
- Transfert de fichiers (FTP)
- Système de noms de domaine (DNS)
- Messagerie électronique (POP3, SMTP et IMAP)
- Partage de fichiers (NFS, SMB)
- Services d'impression (LPD)
- Protocole DHCP (Dynamic Host Configuration Protocol)

Description	NFS	DHCP	HTTP	POP3	FTP	DNS	SMTP	SMB	NAT	LPD
Services Web			✓							
Transfert de fichiers					✓					
Système de noms de domaine (DNS)						✓				
Messagerie électronique				✓			✓			
Partage de fichiers	✓							✓		
Services d'impression										✓
Allocation dynamique d'adresses IP		✓								
Pare-feu									✓	

Service	Protocole TCP/IP
Web	HTTP
Transfert de fichiers	FTP, TFTP
Partage de fichiers	NFS
Messagerie Internet	SMTP, POP3, IMAP
Administration à distance	Telnet
Services d'annuaire (Internet)	DNS, LDAP
Configuration automatique de l'adresse réseau	DHCP
Administration réseau	SNMP

En fonction du système d'exploitation de réseau, certains de ces processus réseau peuvent être activés au cours d'une installation par défaut. La plupart des processus de réseau plébiscités s'appuient sur la suite de protocoles TCP/IP. Comme TCP/IP est un ensemble de protocoles ouvert et bien connu, ses services sont vulnérables aux balayages illicites et aux attaques malveillantes. Les attaques par déni de service, les virus informatiques et les vers Internet à diffusion rapide ont forcé les concepteurs de systèmes d'exploitation de réseau à revoir les services réseau pouvant démarrer automatiquement.

Les dernières versions de systèmes d'exploitation de réseau courants, tels que pour Windows 2000 et Red Hat Linux 7, limitent le nombre de services de réseau activés par défaut. Lors du déploiement d'un système d'exploitation de réseau, les services de réseau stratégiques doivent être activés manuellement.

Quand un utilisateur décide d'imprimer dans un environnement d'impression de réseau, le travail est envoyé à la file d'attente appropriée de l'imprimante sélectionnée. Les files d'attente d'impression empilent les travaux d'impression entrants, puis les exécutent dans leur ordre d'arrivée (FIFO – *First-in, First-out*). Quand un travail est ajouté, il est placé à la fin de la file d'attente et imprimé en dernier. Le délai d'attente de l'impression peut parfois s'avérer long, en fonction de la taille des travaux d'impression situés en tête de la file. Un service d'impression réseau fournit aux administrateurs réseau les outils nécessaires pour gérer le grand nombre de travaux d'impressions routés sur le réseau. Ceci leur permet de changer les priorités, de mettre en pause, voire de supprimer les travaux en attente d'impression.

Partage de fichiers
La possibilité de partager des fichiers en réseau est un important service de réseau. De nombreux protocoles et applications de partage de fichiers s'utilisent de nos jours. Sur un réseau d'entreprise ou familial, on partage généralement les fichiers au moyen de Windows File Sharing ou du protocole NFS. Dans ces environnements, il se peut qu'un utilisateur final ne sache même pas si

un fichier donné réside sur son disque dur local ou sur un serveur distant. Windows File Sharing et NFS permettent aux utilisateurs de déplacer, créer et supprimer en toute facilité des fichiers dans des répertoires distants.

FTP
De nombreuses entreprises mettent des fichiers à la disposition de télétravailleurs, de clients ou du grand public au moyen du protocole FTP. Les services FTP sont à la disposition du public en combinaison avec les services Web. Par exemple, un utilisateur peut naviguer sur un site Web, apprendre l'existence d'une mise à jour logicielle sur une page Web, puis télécharger cette mise à jour à l'aide de FTP. Les sociétés les plus petites peuvent utiliser un serveur unique pour leurs services FTP et HTTP, alors que les entreprises de plus grande taille peuvent opter pour l'utilisation de serveurs FTP dédiés.

Bien que les clients FTP doivent s'identifier, de nombreux serveurs FTP sont configurés pour autoriser les accès anonymes. Quand les utilisateurs accèdent de façon anonyme à un serveur, ils ne leur est pas nécessaire de disposer d'un compte utilisateur sur le système. Le protocole FTP permet aux utilisateurs de télécharger, renommer et supprimer des fichiers et les administrateurs qui souhaitent contrôler les niveaux d'accès doivent donc faire preuve de prudence quand ils configurent un serveur FTP.

Le protocole TCP est orienté connexion. Les clients doivent ouvrir une session de la couche d'application sur le serveur, s'authentifier, puis effectuer une action, telle qu'un téléchargement en amont ou en aval. Si la session du client reste inactive pendant un certain temps, le serveur déconnecte ce client. Cette durée est appelée période d'inactivité. La longueur d'une période d'inactivité FTP est fonction du logiciel.

Services Web
Le World Wide Web est maintenant le service réseau le plus visible. En moins d'une décennie, le World Wide Web est devenu un réseau international pour les informations, le commerce, l'éducation et les loisirs. Des millions de sociétés, d'organisations et de particuliers possèdent des sites Web sur Internet. Les sites Web sont des ensembles de pages Web stockées sur un serveur ou un groupe de serveurs.

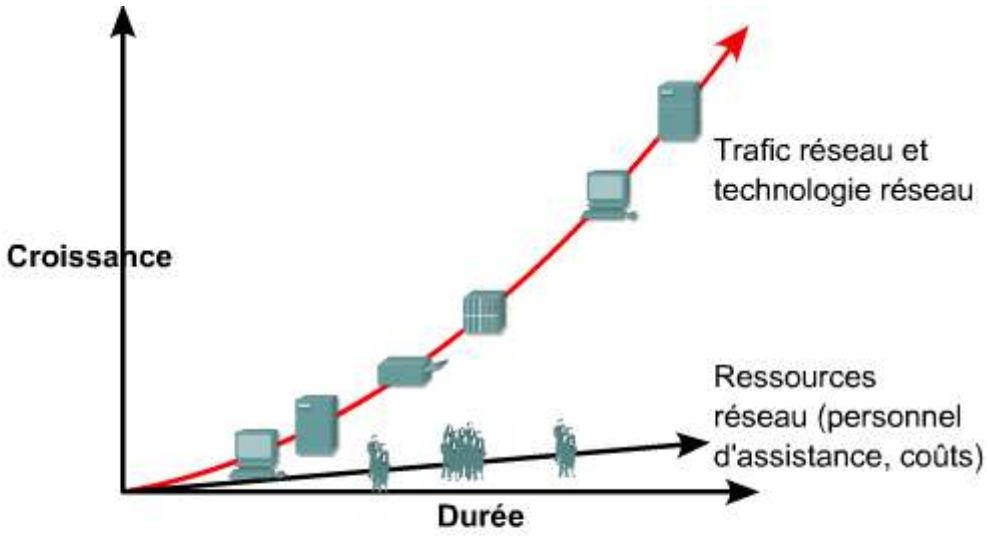
Le World Wide Web est fondé sur un modèle client/serveur. Les clients tentent d'établir des sessions TCP avec des serveurs Web. Une fois qu'une session est établie, un client peut demander des données au serveur. HTTP gère généralement les requêtes des clients et les transferts du serveur. Les logiciels clients Web incluent les navigateurs Web à interface graphique, tels que Netscape Navigator et Internet Explorer.

Les pages Web sont hébergées sur des ordinateurs utilisant des logiciels de service Web. Les logiciels serveurs Web les plus courants sont Microsoft Internet Information Services (IIS) et Apache Web Server. Microsoft IIS tourne sur une plate-forme Windows et Apache Web Server sur des plates-formes UNIX, Linux et Windows. Il existe un logiciel de service Web pour pratiquement tous les systèmes d'exploitation actuellement en production.

DNS
Le protocole DNS traduit un nom Internet, tel que www.cisco.com, en une adresse IP. De nombreuses applications s'appuient sur les services d'annuaire fournis par DNS pour effectuer cette tâche. Les navigateurs Web, les programmes de courrier électronique et de transfert de fichiers utilisent tous les noms des systèmes distants. Le protocole DNS permet à ces clients d'envoyer des requêtes à des serveurs DNS du réseau pour obtenir la traduction de noms en adresses IP. Les applications peuvent ensuite utiliser les adresses pour envoyer leurs messages. Sans ce service d'interrogation d'annuaire, Internet serait pratiquement impossible à utiliser.

DHCP
Le protocole DHCP permet aux ordinateurs individuels d'un réseau IP de récupérer leur configuration TCP/IP sur un ou plusieurs serveurs DHCP. Les serveurs DHCP ne disposent d'aucune information sur les ordinateurs individuels avant que ces informations ne soient demandées. L'objectif global de cette stratégie est de réduire le travail nécessaire à l'administration d'un réseau IP de grande taille. L'information la plus significative distribuée de la sorte est l'adresse IP qui identifie l'hôte sur le réseau. DHCP permet également de récupérer, ainsi que de renouveler automatiquement les adresses IP du réseau par l'intermédiaire d'un mécanisme de bail. Ce mécanisme alloue une adresse IP pendant une période spécifique, la libère, puis alloue une nouvelle adresse IP. Avec le protocole DHCP, c'est un serveur DHCP qui effectue toutes ces activités. L'administrateur système gagne ainsi un temps considérable.

Alors qu'un réseau évolue et s'étend, il devient une ressource de plus en plus cruciale et indispensable pour l'organisation. 1



- À mesure qu'ils s'étendent, les réseaux gagnent également en complexité. Disposer d'une fonctionnalité d'administration est donc une nécessité.
- Les administrateurs réseau ne gèrent plus seulement les éléments de l'infrastructure réseau, mais aussi les services.

À mesure que des ressources réseau sont mises à la disposition des utilisateurs, le réseau devient plus complexe et sa gestion devient plus compliquée. La perte de ressources réseau et les mauvaises performances sont les conséquences de cette augmentation de la complexité et ne sont pas acceptables pour les utilisateurs. 2

Tâches d'administration du réseau

- Facilité d'utilisation
- Capacité de rétablissement
- Contrôle de la disponibilité du réseau
- Automatisation améliorée
- Contrôle des temps de réponse
- Fonctions de sécurité
- Possibilité d'ajouter et de supprimer des utilisateurs
- Réacheminement du trafic
- Enregistrement des utilisateurs

L'administrateur doit gérer activement le réseau, diagnostiquer les problèmes, empêcher certaines situations de survenir et fournir les meilleures performances réseau possibles aux utilisateurs. Il arrive un moment où les réseaux deviennent trop étendus pour être administrés sans outils de gestion automatiques.

L'administration réseau implique les tâches ci-dessous:

- La surveillance de la disponibilité du réseau
- L'amélioration de l'automatisation
- La surveillance des temps de réponse
- La mise en place de fonctionnalités de sécurité
- Le réacheminement du trafic
- Le rétablissement de la fonctionnalité
- L'enregistrement d'utilisateurs

Les forces qui régissent l'administration réseau sont présentées à la figure 3 et expliquées ci-dessous :

Quels sont les facteurs qui rendent nécessaire l'administration réseau ?

- Contrôle des actifs de l'entreprise
- Contrôle de la complexité
- Amélioration du service
- Amélioration de l'automatisation
- Équilibrage des divers besoins
- Réduction des périodes d'indisponibilité
- Contrôle des coûts

- **Contrôle des ressources de l'entreprise** – Si les ressources réseau ne sont pas gérées de façon efficace, elles n'offrent pas les résultats exigés par une bonne administration.
- **Contrôle de la complexité** – Avec la croissance massive du nombre de composants réseau, d'utilisateurs, d'interfaces, de protocoles et de constructeurs, la perte de contrôle du réseau et de ses ressources constitue une menace pour l'administration.
- **Amélioration du service** – Les utilisateurs attendent des services similaires ou améliorés lorsque le réseau s'étend et que les ressources deviennent plus dispersées.
- **Équilibrage des divers besoins** – Diverses applications doivent être mises à la disposition des utilisateurs à un niveau donné de support, avec des exigences spécifiques en termes de performances, de disponibilité et de sécurité.
- **Réduction des temps d'arrêt** – Assurer la haute disponibilité des ressources au moyen d'une conception redondante adéquate.
- **Contrôle des coûts** – Surveillance et contrôle de l'utilisation des ressources, de manière à satisfaire l'utilisateur pour un coût raisonnable.

Certains termes élémentaires d'administration réseau sont présentés à la figure 4

Terme	Définition
SNMP	SNMP (Simple Network Management Protocol) est une norme universelle définie par l'IETF, destinée à la gestion des ressources réseau.
MIB	La base d'informations de management (MIB - Management Information Base) est la structure/la définition des données d'un objet géré.
RMON	RMON (Remote Monitoring) est une spécification d'agent/MIB définissant les fonctions de surveillance des équipements distants.
RFC	Les requêtes pour commentaires (Request For Comments ou RFC) sont des documents émis par l'IETF. Certaines ont été adoptées en tant que normes Internet.
NMS	La station d'administration réseau (Network Management Station) est une station SNMP conçue pour l'administration des équipements réseau. Il s'agit généralement d'une " boîte " UNIX ou NT qui exécute HP Openview, SunNET Mgr ou NetView pour AIX.

.

Activité de média interactive

Glisser-Positionner: Terminologie d'administration réseau

À la fin de cette activité, l'étudiant sera en mesure d'identifier la terminologie utilisée en administration réseau.

6.2 Administration réseau

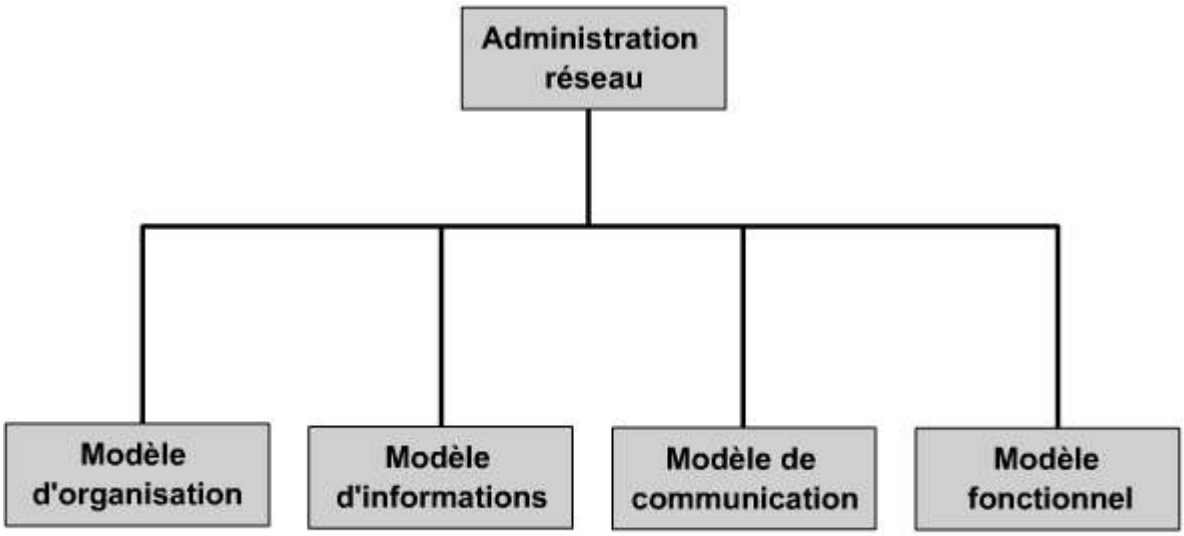
6.2.2 OSI et le modèle d'administration réseau

L'organisme international de normalisation ISO (*International Standards Organization*) a créé un comité visant à produire un modèle pour l'administration réseau, sous la direction du groupe OSI.

Ce modèle se décline en quatre parties:

- Le modèle d'organisation
- Le modèle d'informations
- Le modèle de communication
- Le modèle fonctionnel

Ceci constitue une vue du haut en bas de l'administration réseau, divisée en quatre sous-modèles et reconnue par la norme OSI. 1



Les particularités de chaque modèle dépendent de la norme d'administration réseau adoptée

Le modèle d'organisation 2 décrit les composants de l'administration réseau, par exemple administrateur, agent, et ainsi de suite, avec leurs relations.

- Décrit les composants de l'administration réseau, ainsi que leurs relations.
- Selon les normes, cela peut représenter différents types d'architecture.

La disposition de ces composants mène à différents types d'architecture, décrits plus loin dans ce document.

Le modèle d'informations est relatif à la structure et au stockage des informations d'administration réseau. 3

- Concerne les informations de stockage et de structure
- Représentation des objets et des informations relatives à leur gestion
- L'ISO a défini la règle de gestion des informations d'administration (SMI) pour définir la syntaxe et la sémantique des informations d'administration stockées dans la MIB.

Ces informations sont stockées dans une base de données, appelée base d'informations de management (MIB). L'ISO a établi la structure des informations d'administration (SMI) pour définir la syntaxe et la sémantique des informations d'administration stockées dans la MIB. Les MIB et les SMI sont étudiées en profondeur ultérieurement.

Le modèle de communication traite de la manière dont les données d'administration sont transmises entre les processus agent et administrateur. 4

- Manière dont les données d'administration sont communiquées entre les processus agent et gestionnaire.
- Trois aspects :
  - Moyen de transport de l'échange des messages (protocole de transport)
  - Format de message de la communication (protocole d'application)
  - Message proprement dit (commandes et réponses)

Il est relatif au protocole d'acheminement, au protocole d'application et aux commandes et réponses entre égaux.

Le modèle fonctionnel concerne les applications d'administration réseau qui résident sur la station d'administration réseau (NMS). 5

- Concerne les applications d'administration réseau qui résident sur la station d'administration réseau (NMS)
- Le modèle OSI compte cinq domaines fonctionnels ; il est parfois désigné sous le nom de modèle FCAPS :
  - Panne
  - Configuration
  - Comptabilisation
  - Performances
  - Sécurité

Le modèle d'administration OSI compte cinq domaines fonctionnels, parfois appelés le modèle FCAPS:

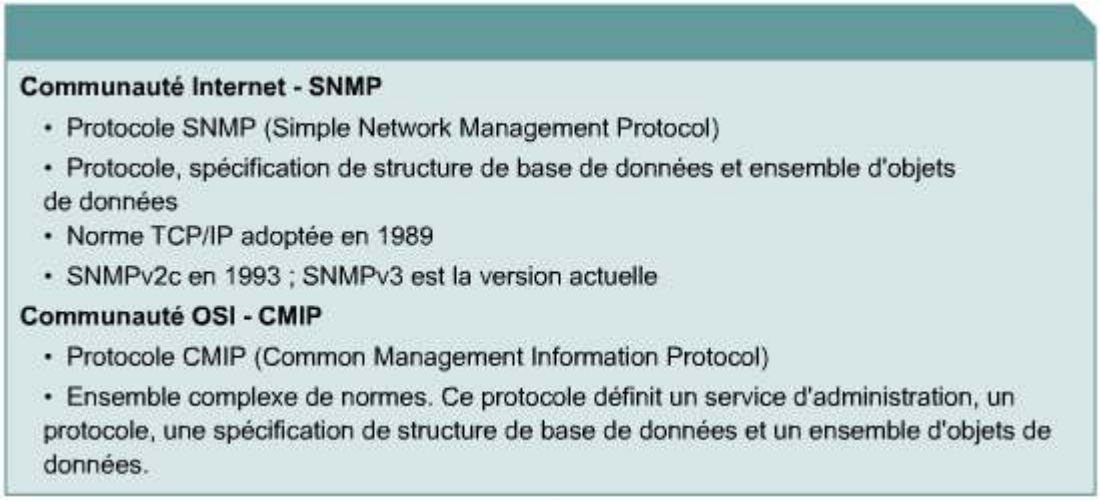
- Les erreurs
- La configuration
- La comptabilité
- Les performances
- La sécurité

Ce modèle d'administration réseau a largement été adopté par les constructeurs au titre de méthode utile de description des besoins de n'importe quel système d'administration réseau.

6.2 Administration réseau

6.2.3 Normes SNMP et CMIP

Pour permettre l'interopérabilité de l'administration sur de nombreuses plates-formes réseau différentes, des normes d'administration s'avèrent nécessaires pour que les constructeurs puissent les mettre en oeuvre et y adhérer. Deux normes principales ont émergé: 1


Communauté Internet - SNMP
• Protocole SNMP (Simple Network Management Protocol)
• Protocole, spécification de structure de base de données et ensemble d'objets de données
• Norme TCP/IP adoptée en 1989
• SNMPv2c en 1993 ; SNMPv3 est la version actuelle
Communauté OSI - CMIP
• Protocole CMIP (Common Management Information Protocol)
• Ensemble complexe de normes. Ce protocole définit un service d'administration, un protocole, une spécification de structure de base de données et un ensemble d'objets de données.

- Le protocole SNMP (*Simple Network Management Protocol*) – Communauté IETF
- Le protocole CMIP (*Common Management Information Protocol*) – Communauté des télécommunications

Le protocole SNMP désigne un ensemble de normes d'administration, notamment un protocole, une spécification de structure de base de données et un ensemble d'objets de données. SNMP a été adopté comme norme pour les réseaux Internet TCP/IP en 1989 et est devenu très populaire. Une mise à niveau, le protocole SNMP version 2c (SNMPv2c) a été adoptée en 1993. SNMPv2c permet de prendre en charge les stratégies d'administration réseau centralisées et distribuées et offre des améliorations au niveau de la structure des informations d'administration (SMI), des opérations de protocole, de l'architecture d'administration et de la sécurité. Il a été conçu pour fonctionner sur les réseaux OSI, ainsi que les réseaux TCP/IP. Depuis, SNMPv3 a été mis en circulation. Pour résoudre les défauts de sécurité de SNMPv1 et SNMPv2c, SNMPv3 fournit un accès sécurisé aux MIB en authentifiant et en cryptant les paquets acheminés sur le réseau. CMIP est un protocole de gestion de réseaux OSI créé et normalisé par l'ISO pour la surveillance et le contrôle de réseaux hétérogènes.

6.2 Administration réseau

6.2.4 Fonctionnement du protocole SNMP

SNMP est un protocole de la couche d'application conçu pour faciliter l'échange d'informations d'administration entre les équipements réseau. En utilisant SNMP pour accéder aux données d'informations d'administration, telles que le nombre de paquets par seconde envoyés sur une interface ou le nombre de connexions TCP ouvertes, les administrateurs réseau peuvent mieux gérer les performances du réseau et mieux rechercher et résoudre les problèmes.

Aujourd'hui, SNMP constitue le protocole le plus répandu pour gérer divers interréseaux commerciaux, universitaires et de recherche.

L'activité de normalisation se poursuit à mesure que les constructeurs développent et mettent sur le marché des applications de pointe d'administration SNMP. SNMP est un protocole simple, mais ses fonctions sont suffisamment efficaces pour gérer les problèmes liés à l'administration des réseaux hétérogènes.

Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments:

- La station d'administration
- L'agent de supervision
- La base d'informations de management
- Le protocole de gestion de réseau

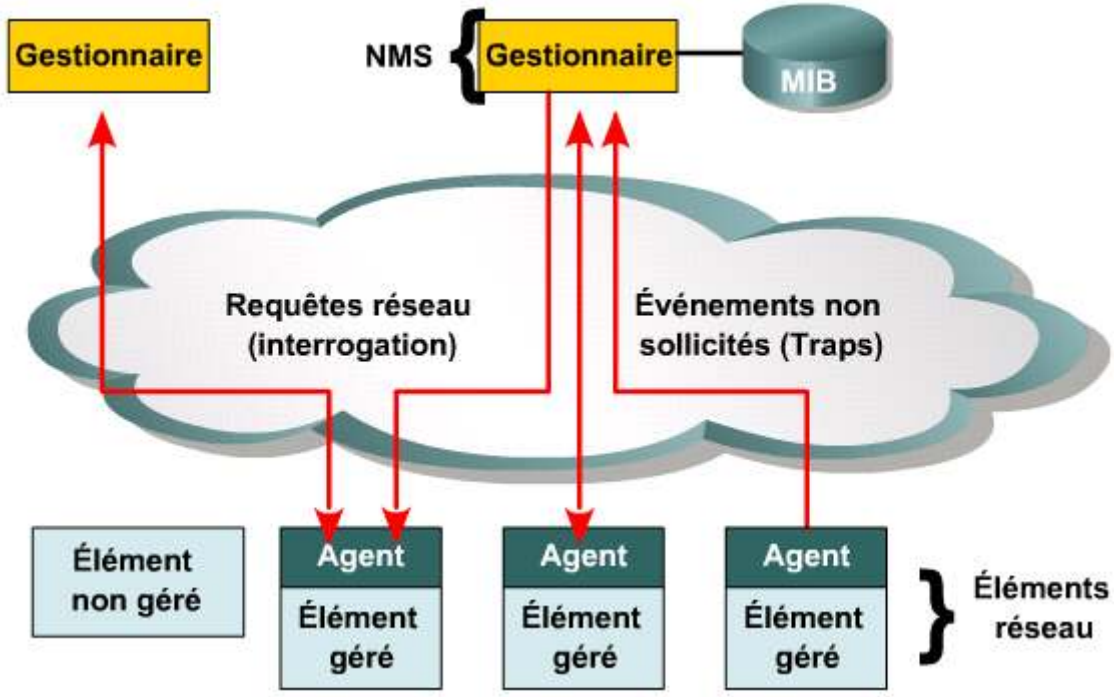
La NMS est généralement une station de travail autonome, mais elle peut être mise en oeuvre sur plusieurs systèmes. Elle contient un ensemble de logiciels appelés l'application d'administration réseau (NMA). La NMA comporte une interface utilisateur permettant aux administrateurs autorisés de gérer le réseau. Elle répond à des commandes utilisateur générées dans l'ensemble du réseau. Les agents de supervision sont des logiciels modulaires résidant dans des équipements de réseau clés tels que d'autres hôtes, routeurs, ponts et concentrateurs. Ils répondent à des requêtes d'informations et des requêtes d'action émises par la NMS, telles que l'interrogation, et peuvent fournir à la NMS des informations très importantes, mais non demandées, telles que les Traps. Toutes les informations de supervision d'un agent en particulier sont stockées dans la base d'informations de management de cet agent. Un agent peut effectuer un suivi des éléments suivants:

- Le nombre et l'état de ses circuits virtuels
- Le nombre de certains types de messages d'erreur reçus
- Le nombre d'octets et de paquets entrant et sortant de l'équipement
- La longueur maximale de la file d'attente de sortie pour les routeurs et autres équipements interréseaux
- Les messages de broadcast envoyés et reçus
- Les interfaces réseau qui se désactivent et s'activent

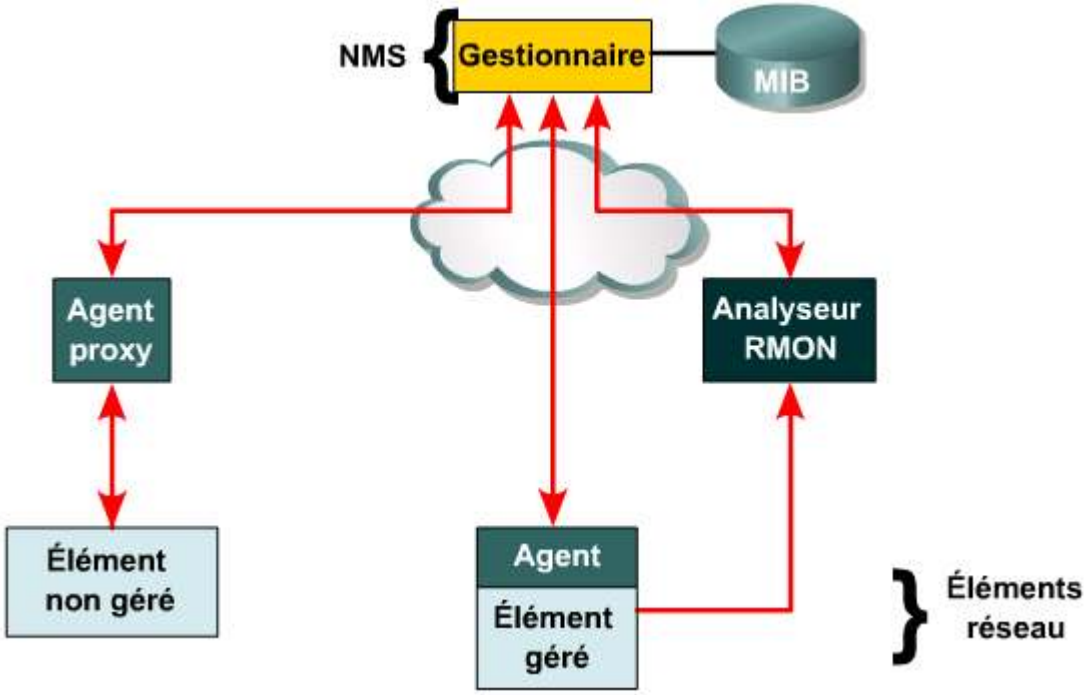
Le NMS exécute une fonction de surveillance en récupérant les valeurs dans la MIB. La NMS peut occasionner l'exécution d'une action au niveau d'un agent. La communication entre la station d'administration et l'agent est réalisée par un protocole d'administration réseau de la couche d'application. Le protocole SNMP utilise le protocole UDP (*User Datagram Protocol*) et communique sur les ports 161 et 162. Il est fondé sur un échange de messages. Il existe trois types de message courants:

- **Get** – Permet à la station d'administration de récupérer la valeur des objets MIB à partir de l'agent.
- **Set** – Permet à la station d'administration de définir la valeur des objets MIB au niveau de l'agent.
- **Trap** – Permet à l'agent d'avertir la station d'administration lors d'événements significatifs.

Ce modèle est appelé modèle à deux niveaux. 1



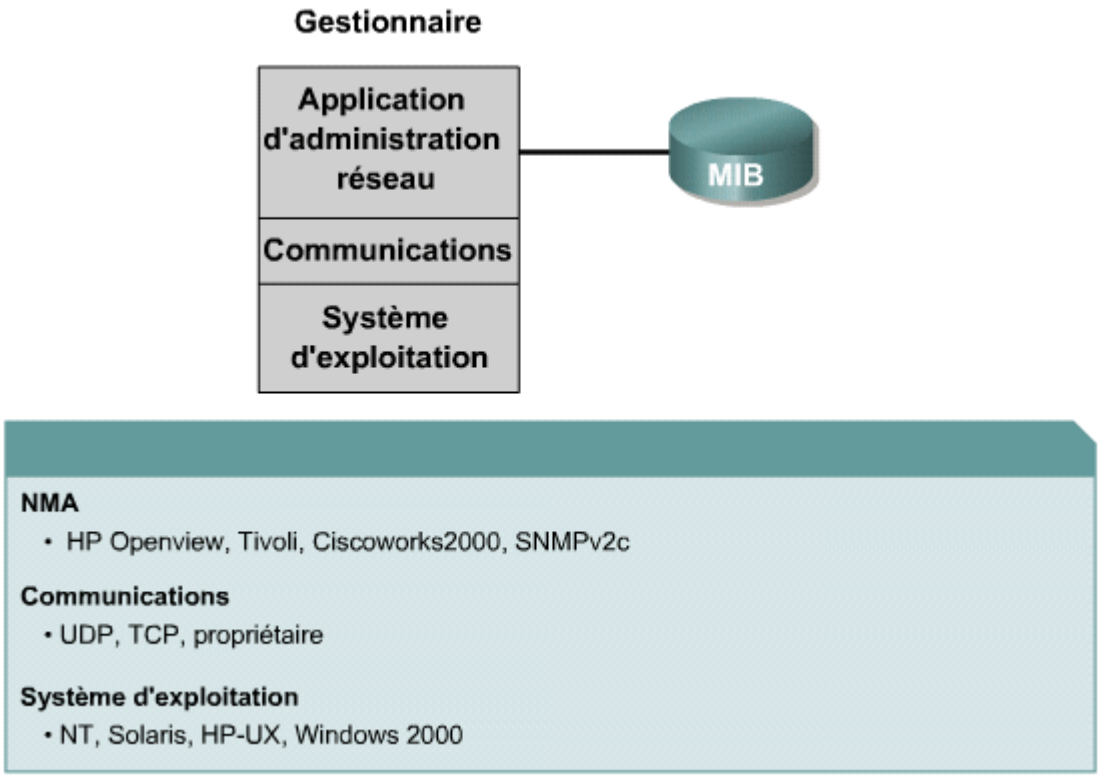
Toutefois, il présuppose que tous les éléments du réseau peuvent être administrés par SNMP. Cela n'est pas toujours le cas, car certains équipements disposent d'une interface d'administration propriétaire. Dans ces cas de figure, un modèle à trois niveaux s'avère nécessaire. 2



Une station d'administration réseau qui souhaite obtenir des informations ou contrôler ce nœud propriétaire communique avec un agent proxy. L'agent proxy traduit alors la requête SNMP de la station d'administration en un formulaire approprié au système cible, puis utilise le protocole d'administration propriétaire approprié pour communiquer avec ce système cible. Les réponses entre la cible et le proxy sont traduites en messages SNMP et renvoyées à la station d'administration.

Les applications d'administration réseau déchargent souvent des fonctionnalités de gestion réseau à un analyseur distant (RMON). Cet analyseur RMON recueille localement des informations d'administration, puis la station d'administration réseau récupère régulièrement un résumé de ces données.

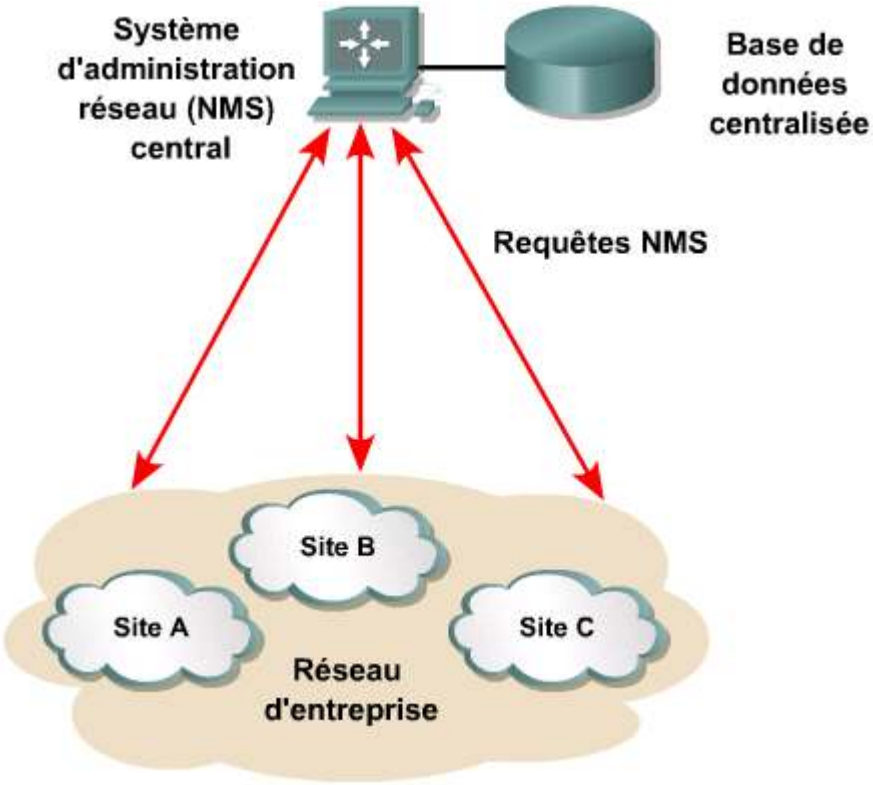
La NMS est une station de travail ordinaire, utilisant un système d'exploitation classique. 3



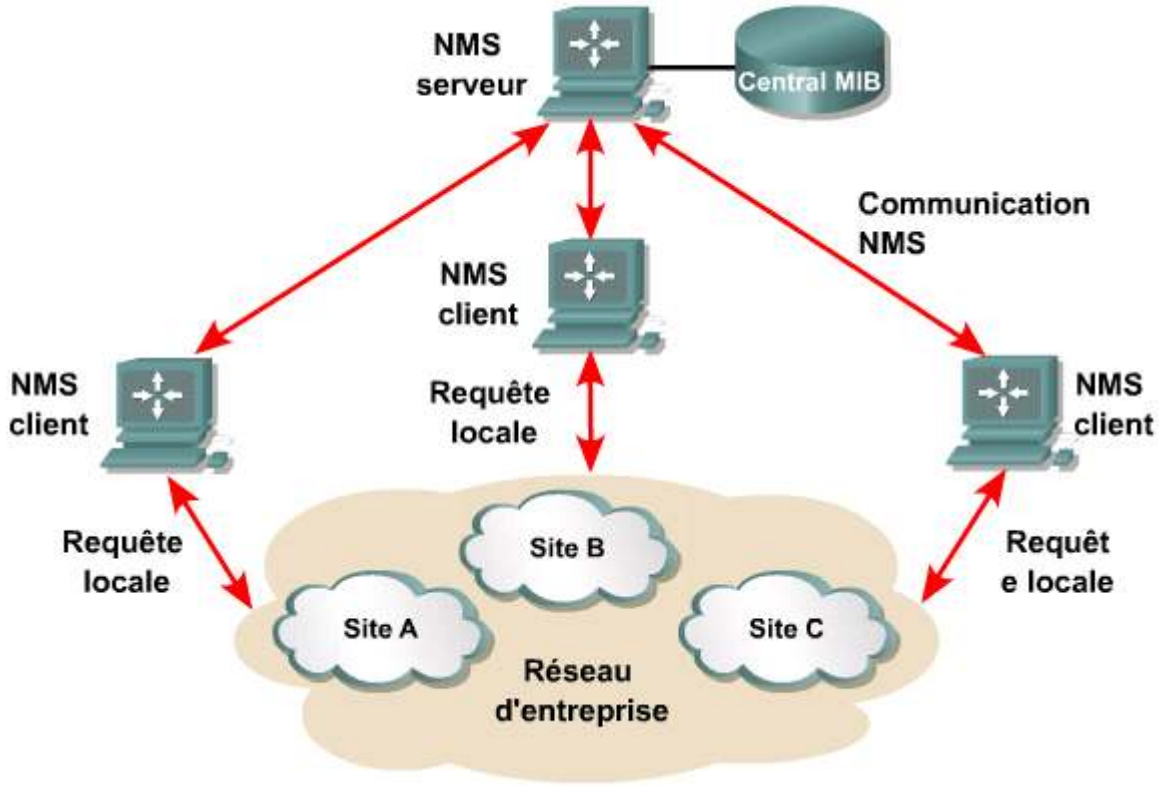
Elle dispose d'une grande quantité de mémoire vive, qui lui permet d'héberger toutes les applications d'administration exécutées simultanément. La station d'administration utilise une pile de protocoles de réseau typique, telle que TCP/IP. Les applications

d'administration réseau s'appuient sur le système d'exploitation hôte et sur l'architecture de communication. Les applications d'administration réseau peuvent, par exemple, être Ciscoworks2000, HP Openview et IBM NetView.

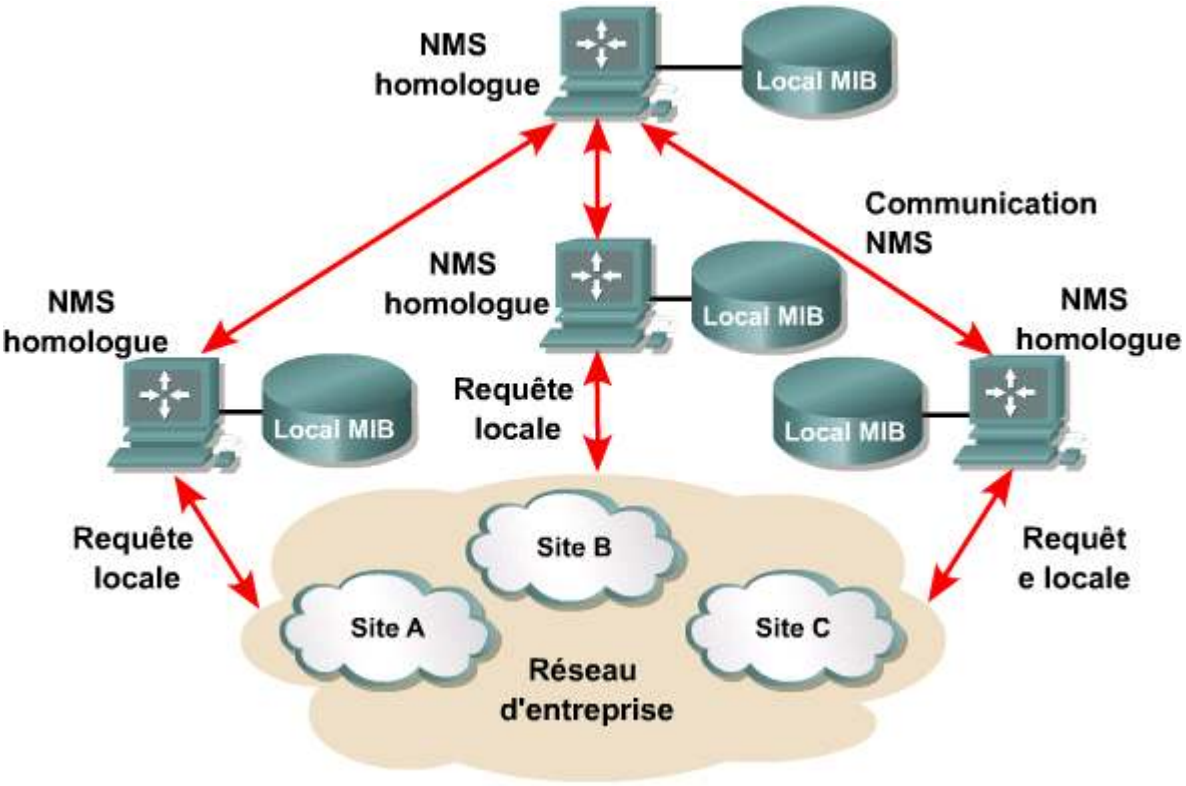
Comme mentionné précédemment, la station d'administration peut être une station de travail autonome centralisée qui envoie des requêtes à tous les agents, quel que soit leur emplacement. 4



Dans un réseau distribué, une architecture décentralisée s'avère plus appropriée, avec une NMS locale au niveau de chaque site. Ces NMS distribuées peuvent fonctionner dans une architecture client-serveur, dans laquelle une NMS sert de serveur maître et les autres de clients. Les clients envoient leurs données au serveur maître pour centraliser le stockage. 5



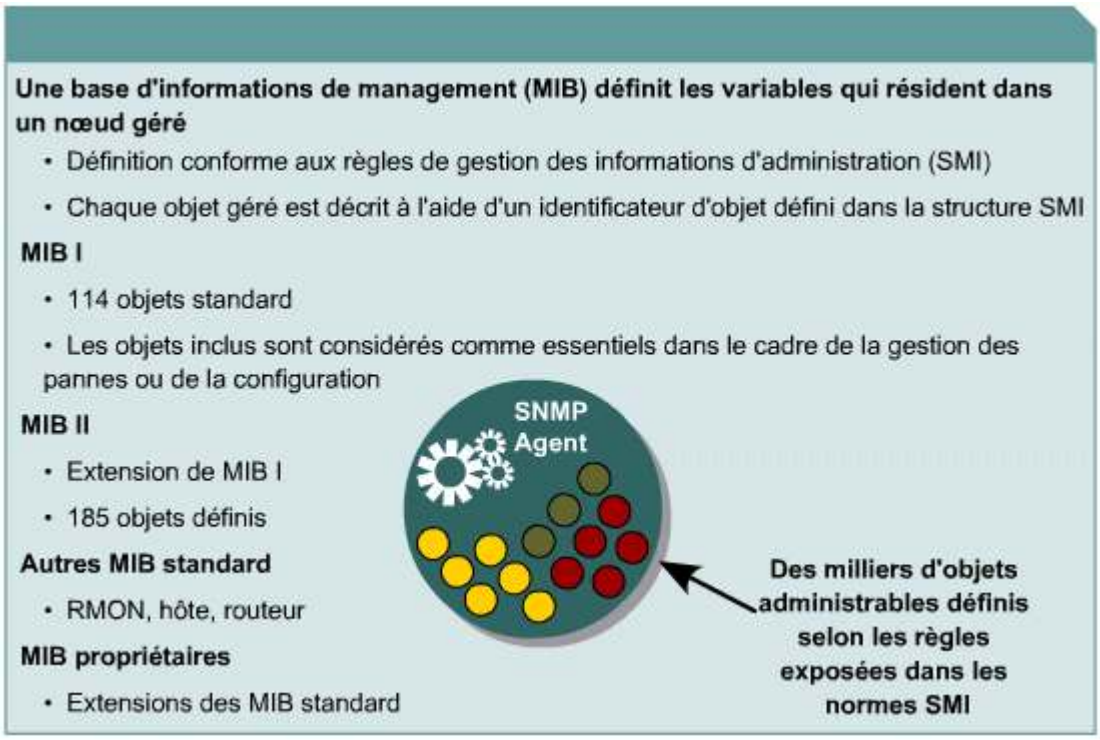
Une autre possibilité consiste à attribuer une responsabilité égale à toutes les NMS distribuées, chacune disposant de ses propres bases de données de management, de telle sorte que les informations d'administration soient distribuées sur les NMS homologues. 6



6.2 Administration réseau

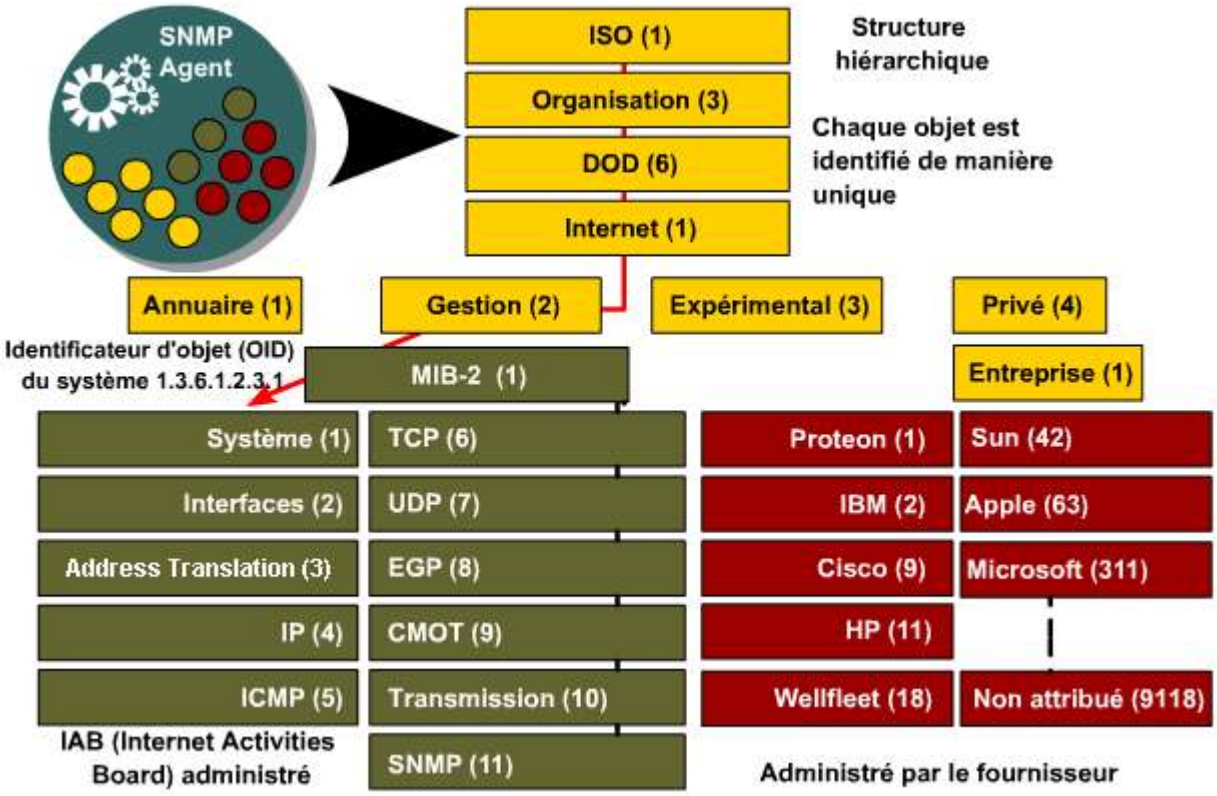
6.2.5 Structure des informations d'administration et des MIB

Une MIB permet de stocker les informations structurées représentant les éléments de réseau et leurs attributs. La structure par elle-même est définie dans une norme dénommée SMI, qui définit les types de données pouvant être utilisés pour stocker un objet, la manière dont ces objets sont nommés et celle dont ils sont cryptés pour être transmis sur un réseau. 1


Une base d'informations de management (MIB) définit les variables qui résident dans un nœud géré
• Définition conforme aux règles de gestion des informations d'administration (SMI)
• Chaque objet géré est décrit à l'aide d'un identificateur d'objet défini dans la structure SMI
MIB I
• 114 objets standard
• Les objets inclus sont considérés comme essentiels dans le cadre de la gestion des pannes ou de la configuration
MIB II
• Extension de MIB I
• 185 objets définis
Autres MIB standard
• RMON, hôte, routeur
MIB propriétaires
• Extensions des MIB standard
SNMP Agent
Des milliers d'objets administrables définis selon les règles exposées dans les normes SMI

Les MIB sont des référentiels très structurés d'informations concernant un équipement. Il existe de nombreuses bases MIB standard, mais il existe un plus grand nombre encore de MIB propriétaires, conçues pour administrer exclusivement les équipements de différents constructeurs. La MIB SMI d'origine a été subdivisée en huit groupes différents, pour un total de 114 objets administrés. D'autres groupes ont été ajoutés pour définir MIB-II, qui remplace désormais MIB-I.

Tous les objets administrés de l'environnement SNMP sont organisés en une structure hiérarchique ou arborescente. Les objets feuille de l'arborescence, c'est-à-dire les éléments qui apparaissent dans le bas du diagramme, sont les objets administrés. Chaque objet administré représente une ressource, une activité ou une information associée à gérer. Un identificateur d'objet unique, à savoir un nombre en notation séparée par des points, identifie chaque objet administré. Chaque identificateur d'objet est décrit en notation de syntaxe abstraite (ASN.1). 2



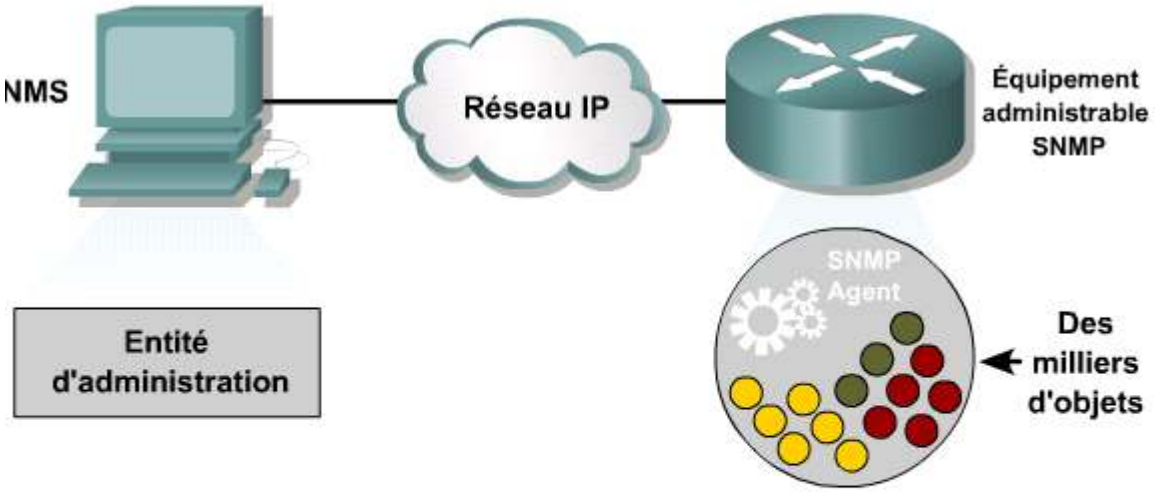
Le protocole SNMP utilise ces identificateurs d'objet pour identifier les variables MIB à récupérer ou à modifier. Les objets dans le domaine public sont décrits dans les présentations des MIB fournies dans les requêtes pour commentaires (RFC). Celles-ci peuvent facilement être consultées à l'adresse: http://www.ietf.org

Tous les constructeurs sont encouragés à faire connaître leurs définitions de MIB. Une fois qu'une valeur d'entreprise assignée a été fournie, le constructeur est responsable de la création et de la gestion des sous-arborescences.

6.2 Administration réseau

6.2.6 Protocole SNMP

L'agent est une fonction logicielle intégrée à la plupart des équipements de réseau, tels que les routeurs, les commutateurs, les concentrateurs administrés, les imprimantes et les serveurs. 1

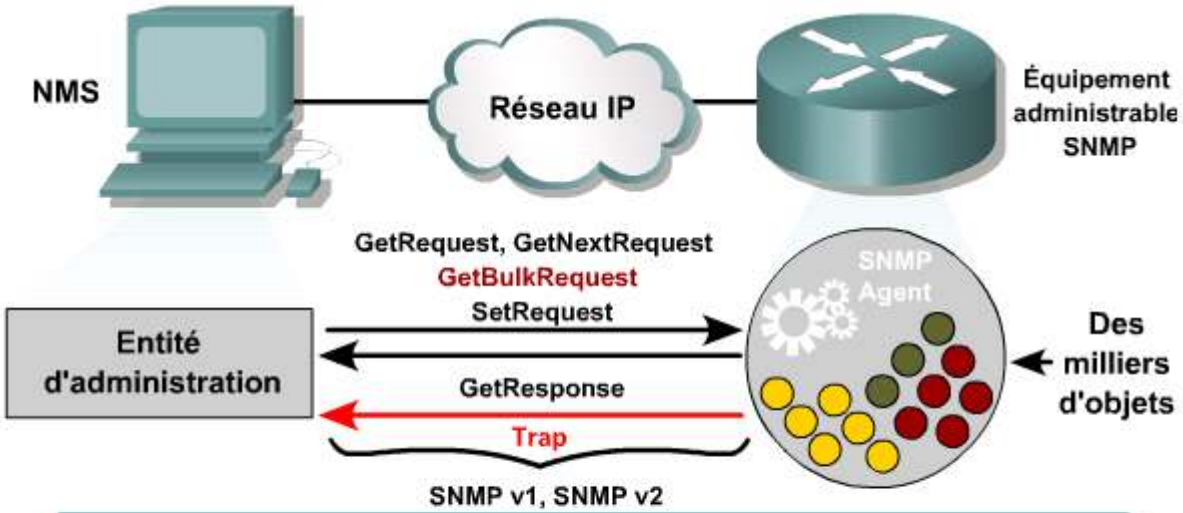


- Entrepôt d'informations
- Structuration des informations conformément aux règles de gestion des informations d'administration (SMI)
- Définitions d'objets fournies dans de nombreuses bases d'informations de management (MIB)

Il est responsable du traitement des requêtes SNMP provenant de la station d'administration. Il est également responsable de l'exécution de routines de gestion de variables définies dans les diverses bases MIB prises en charge.

L'interaction entre la station d'administration et l'agent est facilitée par le protocole SNMP. Le terme « simple » vient du nombre limité de types de messages faisant partie de la spécification initiale du protocole. La stratégie a été conçue pour faciliter aux développeurs l'établissement de fonctions d'administration dans les équipements de réseau. La spécification initiale du protocole est désignée par l'acronyme SNMPv1 (version 1).

Trois types de messages SNMP sont émis pour une NMS. Il s'agit des messages GetRequest, GetNextRequest et SetRequest. 2

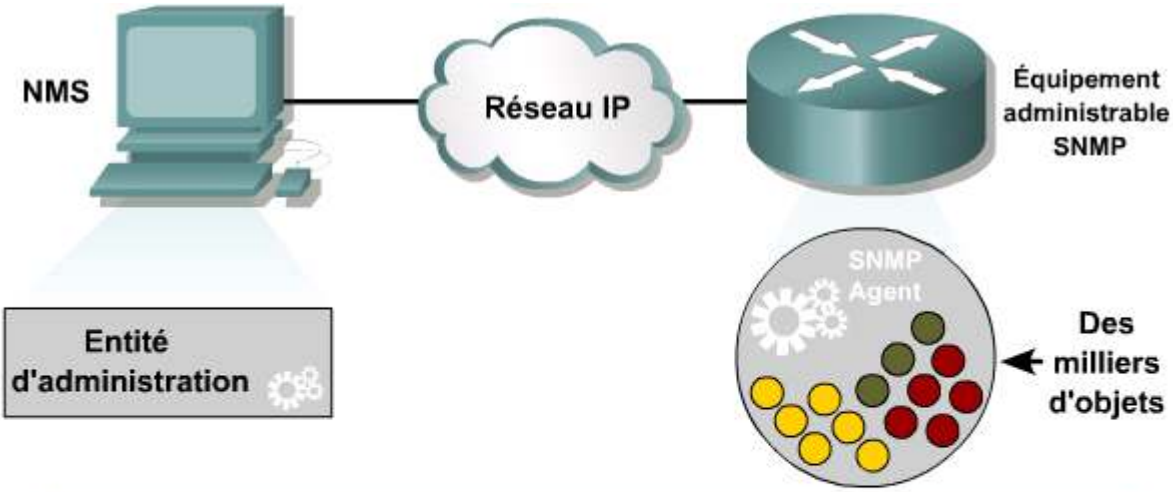


- Commande GetRequests utilisée pour lire la valeur de l'objet
- Commande SetRequests utilisée pour modifier la valeur de l'objet
- Les messages Trap permettent une notification d'événements asynchrone

Ces trois messages sont reconnus par l'agent sous la forme d'un message GetResponse. Un agent peut émettre un message de Trap en réponse à un événement agissant sur la MIB et sur les ressources sous-jacentes.

Le développement de SNMPv2c a permis de résoudre certaines limitations de SNMPv1. L'amélioration la plus remarquable a été l'introduction du type de message GetBulkRequest et l'ajout de compteurs sur 64 bits à la MIB. La récupération d'informations à l'aide de GetRequest et de GetNextRequest constituait une méthode peu efficace de collecte. Avec SNMPv1, il était seulement possible de solliciter une variable à la fois. GetBulkRequest résout cette faiblesse en permettant de recevoir plus d'informations à la suite d'une seule requête. Deuxièmement, les compteurs sur 64 bits résolvent le problème des compteurs à la rotation trop rapide, en particulier avec des liaisons à vitesse élevée telles que Gigabit Ethernet.

L'entité d'administration est également appelée station d'administration ou NMS. 3



- L'entité d'administration recueille des données en générant des requêtes. Cela entraîne la coexistence du trafic in-band et du trafic de production.
- L'entité d'administration reçoit des notifications d'alarmes réseau ou d'événements. Ces notifications peuvent être retransmises au gestionnaire par courrier électronique ou par SMS.
- L'entité d'administration exécute des applications afin d'analyser ou d'interpréter les données de gestion.

C'est elle qui est responsable de la sollicitation d'informations auprès de l'agent. Les sollicitations sont fondées sur des requêtes très spécifiques. La station d'administration dispose de plusieurs méthodes pour traiter les informations récupérées. Ces informations récupérées peuvent être consignées en vue d'une analyse ultérieure, affichées dans un utilitaire graphique, ou comparées à des valeurs préconfigurées pour vérifier si une condition en particulier a été remplie.

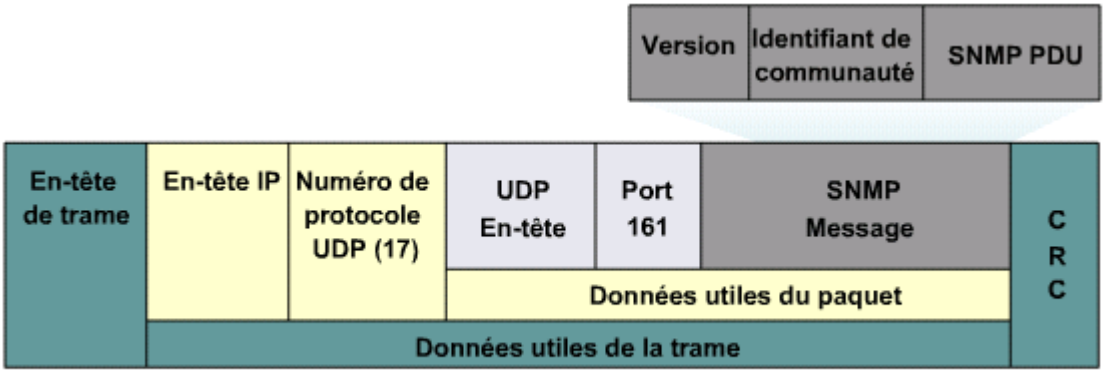
La station d'administration ne sert pas seulement à récupérer des données. Elle comporte également une fonction permettant de modifier une valeur sur l'équipement administré. Cette fonctionnalité permet à un administrateur de configurer un équipement au moyen du protocole SNMP.

L'interaction entre la station d'administration et l'équipement administré occasionne du trafic sur le réseau. Il est donc recommandé d'être prudent lorsque lors de l'introduction des stations d'administration sur le réseau. Les stratégies de surveillance trop agressives peuvent nuire aux performances du réseau. La bande passante est alors plus sollicitée, ce qui peut constituer un problème dans les environnements de WAN. Par ailleurs, la surveillance a un impact sur les performances des équipements surveillés, puisque ceux-ci sont censés traiter les requêtes de la station d'administration. Ce traitement ne doit pas prendre la priorité sur les services de production.

En règle générale, une quantité minimale d'informations doit être interrogée aussi rarement que possible. Déterminez les équipements et les liaisons les plus stratégiques, ainsi que le type de données nécessaire.

Le protocole SNMP utilise le protocole d'acheminement UDP (User Diagram Protocol). Étant donné qu'UDP fonctionne sans connexion et n'est pas fiable, il se peut que le protocole SNMP perde des messages. Le protocole SNMP lui-même n'est pas censé garantir la livraison et c'est donc l'application utilisant SNMP qui doit s'occuper des messages perdus.

Chaque message SNMP contient une chaîne en texte clair, que l'on appelle identifiant de communauté. L'identifiant de communauté s'utilise comme un mot de passe pour limiter l'accès aux équipements administrés. 4



Les unités de données de protocole (PDU) SNMP sont traitées conformément à la politique d'accès indiquée par l'identifiant de communauté.

Les identifiants de communauté sont en texte clair. Ils fournissent un mécanisme d'authentification de base.

(SNMP v1, v2c)

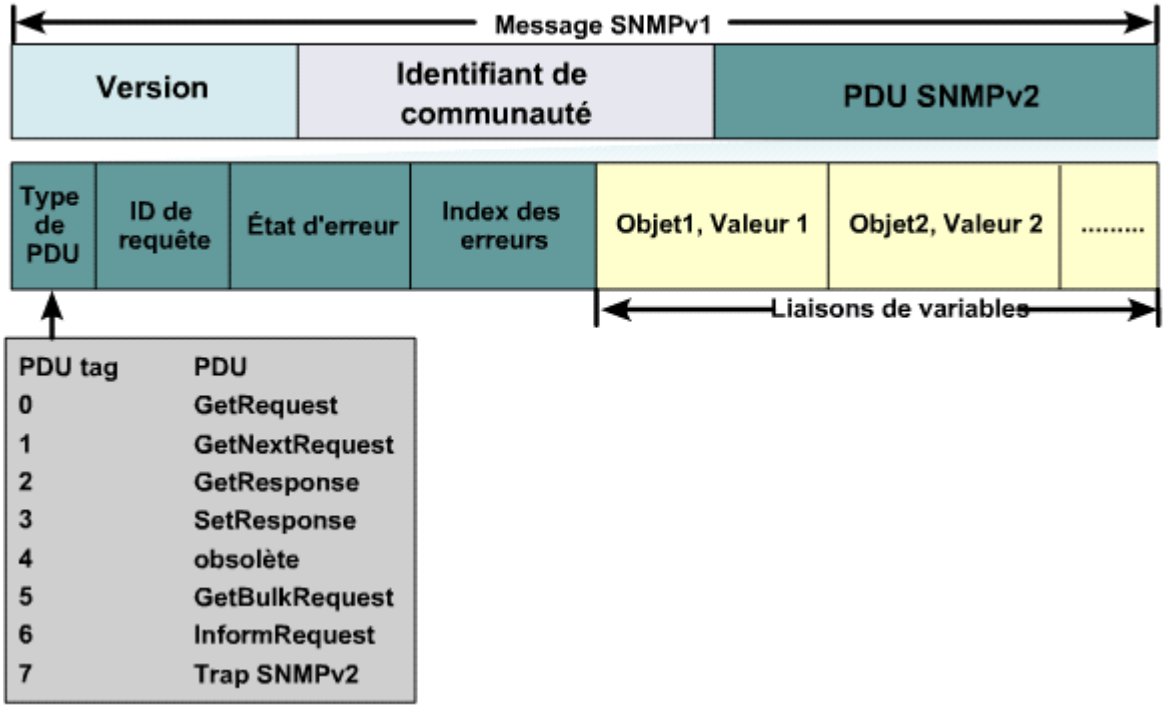
Évitez d'attribuer à l'identifiant de communauté des valeurs par défaut bien connues :

- Accès à l'agent en lecture seule : public
- Accès à l'agent en lecture/écriture : privé

SNMPv3 a résolu les préoccupations de sécurité mises en évidence par la transmission de l'identifiant de communauté en texte clair.

Un exemple de message SNMPv2c est présenté à la figure 5.

SNMPv2c utilise des PDU SNMPv2, mais les encapsule au format SNMPv1



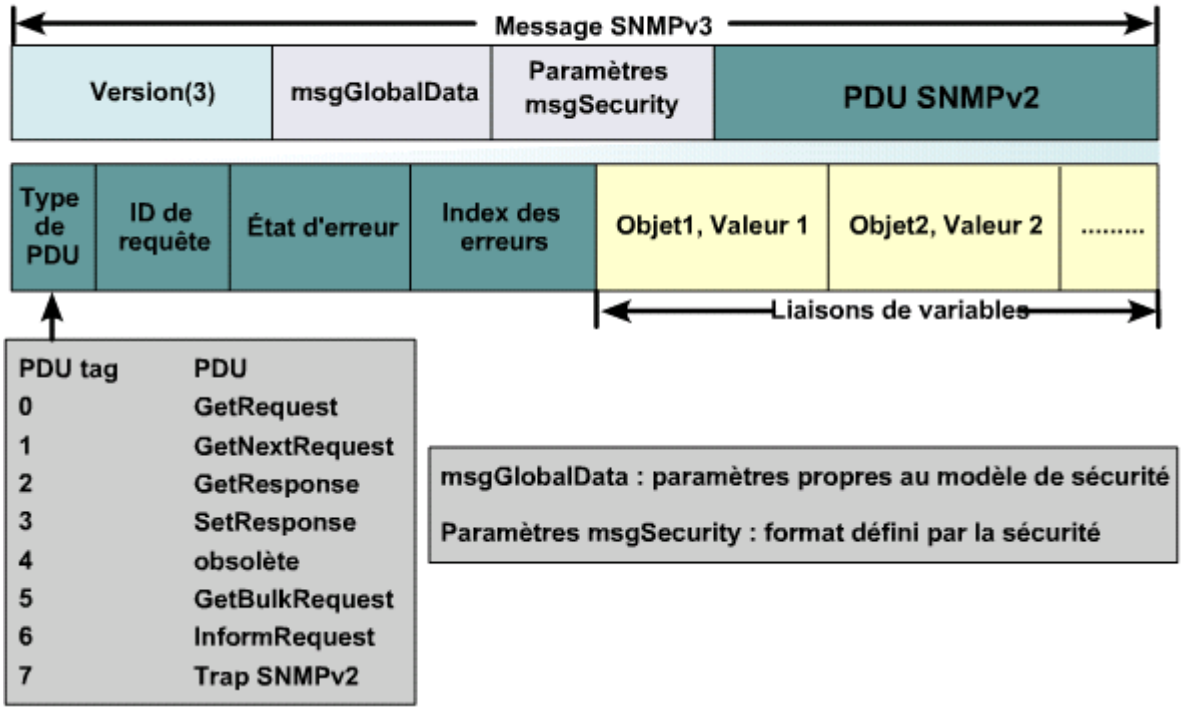
Une présentation détaillée du protocole est fournie dans la norme Internet RFC1905.

Le fait que cette chaîne de communauté soit en texte clair n'est pas surprenant pour quiconque a étudié la suite de protocoles IP (*Internet Protocol*). En effet, tous les champs spécifiés dans cette suite de protocoles sont en texte clair, à l'exception des spécifications d'authentification et de cryptage.

L'identificateur de communauté était essentiellement une marque de réservation de sécurité jusqu'à ce que le groupe de travail SNMPv2 puisse ratifier les mécanismes de sécurité. Les efforts étaient présentés au groupe de travail SNMPv3. Toutes les applications d'administration SNMP doivent être configurées avec les identificateurs de communauté appropriés. Certaines entreprises modifient fréquemment les valeurs de leurs identificateurs de communauté pour réduire les risques d'activités malveillantes entraînées par une utilisation non autorisée du service SNMP.

Malgré la faiblesse associée à l'authentification par communauté, les stratégies d'administration s'appuient toujours sur SNMPv1. Les équipements Cisco prennent en charge les types de message et les fonctions de sécurité enrichies de SNMPv3, mais la plupart des logiciels d'administration ne gèrent pas SNMPv3. 6

SNMPv3 utilise des PDU SNMPv2, mais les encapsule au format SNMPv3



SNMPv3 accepte l'existence simultanée de plusieurs modèles de sécurité. 7

	Niveau	Auth	Cryptage	Que se passe-t-il ?
SNMPv1	noAuthNoPriv	Identifiant de communauté		Utilise la correspondance des identifiants de communauté pour l'authentification
SNMPv2c	noAuthNoPriv	Identifiant de communauté		Utilise la correspondance des identifiants de communauté pour l'authentification
SNMPv3	noAuthNoPriv	Nom d'utilisateur		Utilise la correspondance des identifiants de nom d'utilisateur pour
SNMPv3	authNoPriv	MD5 or SHA		Authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA
SNMPv3	authPriv	MD5 or SHA	DES	Cryptage DES 56 bits en plus de l'authentification basée sur DES-56

Pour que la NMS puisse communiquer avec les équipements en réseau, SNMP doit être activé et les identificateurs de communauté SNMP doivent être configurés sur ces équipements. Pour configurer ces derniers, on utilise la syntaxe de ligne de commande présentée aux paragraphes ci-après.

Plusieurs chaînes en lecture seule sont prises en charge. Sur la plupart des systèmes, la valeur par défaut de cet identificateur de communauté est « public ». Il est déconseillé d'utiliser la valeur par défaut dans un réseau d'entreprise. Pour configurer l'identificateur de communauté en lecture seule utilisé par l'agent, utilisez la commande ci-dessous: 1

Spécification de l'identifiant de communauté en lecture seule

```
Router(config)#snmp-server community string ro
```

Spécification de l'identifiant de communauté en lecture/écriture

```
Router(config)#snmp-server community string rw
```

Spécification de l'emplacement et du contact principal de l'équipement géré

```
Router(config)#snmp-server location text
Router(config)#snmp-server contact text
```

```
Router(config)#snmp-server community stringro
```

- *String* – Identificateur de communauté servant de mot de passe et autorisant l'accès au protocole SNMP.
- **ro** – (Facultatif) Spécifie un accès en lecture seule. Les stations d'administration autorisées peuvent seulement récupérer des objets de la MIB.

Plusieurs chaînes en lecture-écriture sont prises en charge. Tous les objets SNMP sont disponibles pour un accès en écriture. Sur la plupart des systèmes, la valeur par défaut de cet identificateur de communauté est « private ». Il est déconseillé d'utiliser cette valeur dans un réseau d'entreprise. Pour configurer l'identificateur de communauté en lecture-écriture utilisé par l'agent, utilisez la commande ci-dessous :

```
Router(config)#snmp-server community stringrw
```

- **rw** – (Facultatif) Spécifie un accès en lecture-écriture. Les stations d'administration autorisées peuvent récupérer et modifier les objets de la MIB.

Plusieurs chaînes peuvent être utilisées pour indiquer l'emplacement de l'équipement administré et le contact du système principal pour cet équipement.

```
Router(config)#snmp-server location text
Router(config)#snmp-server contact text
```

- *text* – Chaîne décrivant les informations d'emplacement du système

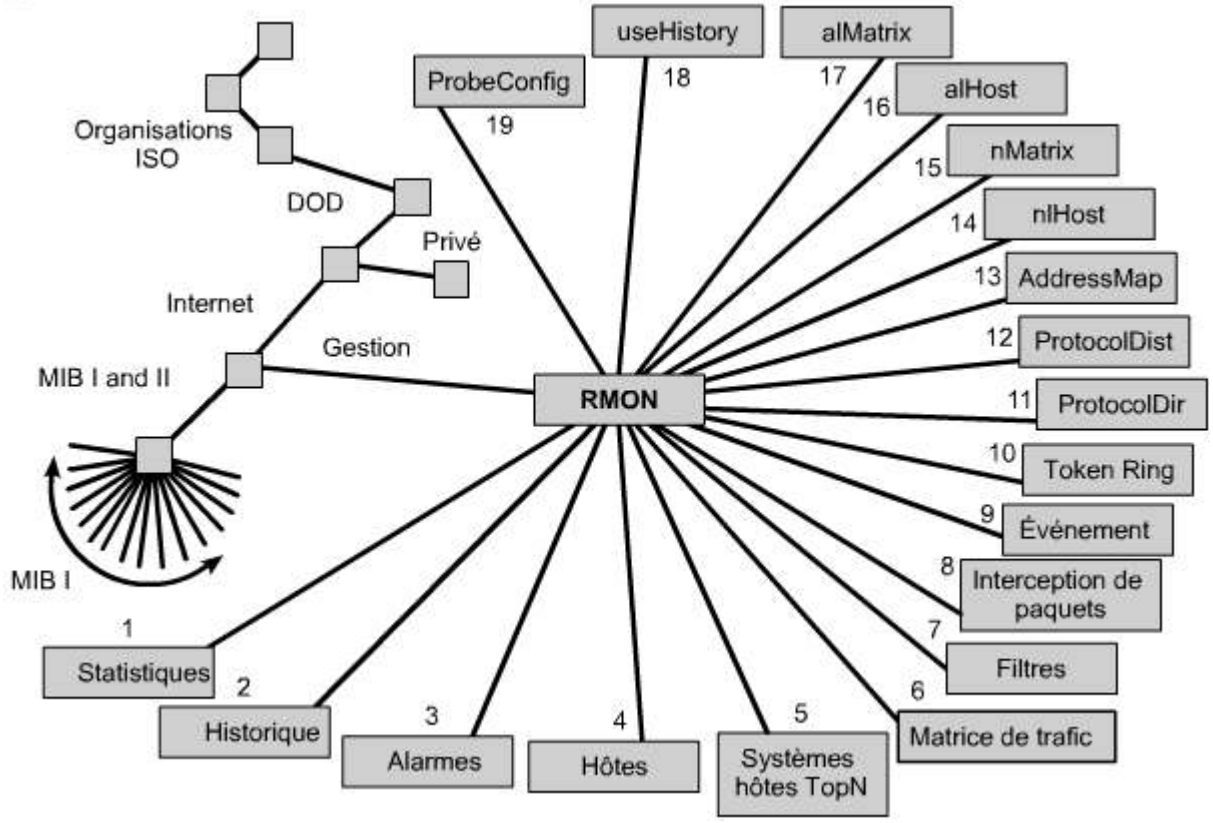
Ces valeurs sont stockées dans les objets MIB *sysLocation* et *sysContact*.

6.2.8 RMON

L'analyseur RMON représente un grand pas en avant dans l'administration d'interréseaux. Il définit une MIB de surveillance à distance qui complète MIB-II et fournit à l'administrateur des informations précieuses sur le réseau. RMON offre la caractéristique remarquable de n'être qu'une spécification d'une MIB, sans modification du protocole SNMP sous-jacent, mais qui permet d'étendre considérablement la fonctionnalité SNMP. 1

- RMON est une MIB
- RMON est basé sur les RFC de l'IETF
- Rassemblement de statistiques en analysant chaque trame sur un segment
- RMON1 est destiné à la couche liaison de données
- RMON2 est adapté pour les couches 3 (réseau) à 7 (application)
- Compatibilité avec un analyseur externe ou un module d'analyse réseau sur Catalyst

Avec MIB-II, l'administrateur réseau peut obtenir des informations qui sont purement locales à certains équipements individuels. 2



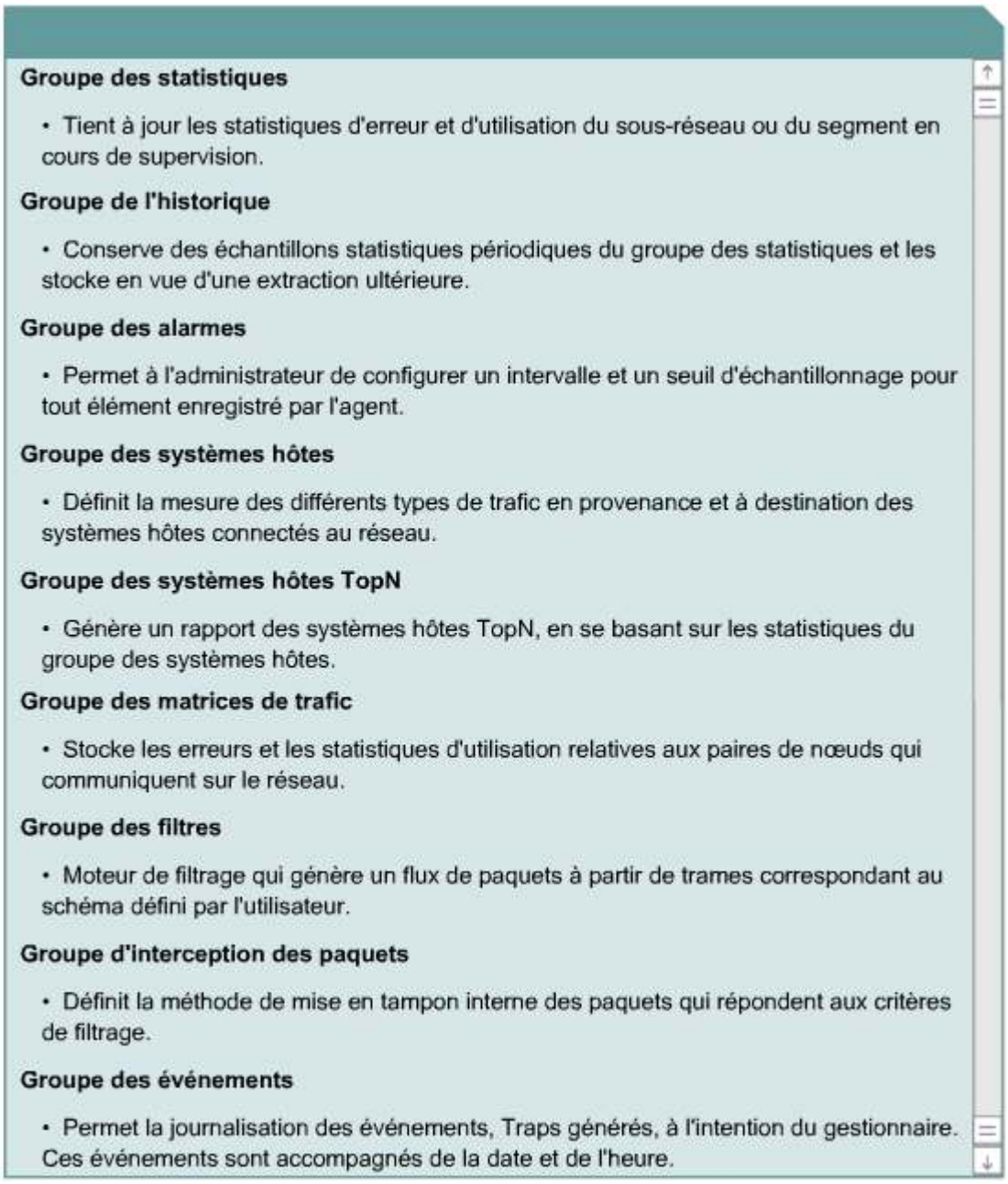
Imaginons un réseau local comprenant plusieurs équipements, chacun d'entre eux doté d'un agent SNMP. Une station d'administration SNMP peut recevoir des informations sur la quantité de trafic entrant et sortant de chaque équipement, mais avec MIB-II, elle ne peut pas être informée facilement du trafic global du réseau local.

L'administration réseau dans un environnement d'interréseaux nécessite généralement un moniteur par sous-réseau.

La norme RMON, à l'origine appelée IETF RFC 1271, et maintenant RFC 1757, a été conçue pour fournir une surveillance et des diagnostics proactifs aux réseaux locaux distribués. Des dispositifs de surveillance, appelés agents ou analyseurs, placés sur des segments stratégiques du réseau permettent de créer des alarmes définies par l'utilisateur, ainsi que de rassembler une multitude de statistiques vitales grâce à l'analyse de chaque trame d'un segment.

La norme RMON répertorie les fonctions de surveillance dans neuf groupes correspondant aux topologies Ethernet, plus un dixième dans RFC 1513 pour les paramètres spécifiques à Token Ring. La norme RMON a été développée dans le but d'être déployée comme une architecture distribuée dans laquelle les agents et les analyseurs communiquent avec une station d'administration centralisée, c'est-à-dire un client, au moyen du protocole SNMP. Ces agents ont défini des structures MIB

SNMP pour les neuf ou dix groupes RMON Ethernet ou Token Ring, ce qui permet une interopérabilité entre les constructeurs d'outils de diagnostic RMON. Les groupes RMON sont définis ci-dessous: 3


Groupe des statistiques
• Tient à jour les statistiques d'erreur et d'utilisation du sous-réseau ou du segment en cours de supervision.
Groupe de l'historique
• Conserve des échantillons statistiques périodiques du groupe des statistiques et les stocke en vue d'une extraction ultérieure.
Groupe des alarmes
• Permet à l'administrateur de configurer un intervalle et un seuil d'échantillonnage pour tout élément enregistré par l'agent.
Groupe des systèmes hôtes
• Définit la mesure des différents types de trafic en provenance et à destination des systèmes hôtes connectés au réseau.
Groupe des systèmes hôtes TopN
• Génère un rapport des systèmes hôtes TopN, en se basant sur les statistiques du groupe des systèmes hôtes.
Groupe des matrices de trafic
• Stocke les erreurs et les statistiques d'utilisation relatives aux paires de nœuds qui communiquent sur le réseau.
Groupe des filtres
• Moteur de filtrage qui génère un flux de paquets à partir de trames correspondant au schéma défini par l'utilisateur.
Groupe d'interception des paquets
• Définit la méthode de mise en tampon interne des paquets qui répondent aux critères de filtrage.
Groupe des événements
• Permet la journalisation des événements, Traps générés, à l'intention du gestionnaire. Ces événements sont accompagnés de la date et de l'heure.

- **Groupe de statistiques** – Tient à jour les statistiques d'erreur et d'utilisation du sous-réseau ou du segment en cours de supervision. Il s'agit, par exemple, de l'utilisation de la bande passante, du broadcast, du multicast, de l'alignement CRC, des fragments, et ainsi de suite.
- **Groupe de l'historique** – Conserve des échantillons statistiques périodiques du groupe des statistiques et les stocke en vue d'une extraction ultérieure. Il s'agit, par exemple, de l'utilisation, du nombre d'erreurs et du nombre de paquets.
- **Groupe des alarmes** – Permet à l'administrateur de configurer l'intervalle et le seuil d'échantillonnage pour tout élément enregistré par l'agent. Il s'agit, par exemple, des valeurs absolues et relatives, ou des seuils en augmentation ou en diminution.
- **Groupe des systèmes hôtes** – Définit la mesure des différents types de trafic en provenance et à destination des systèmes hôtes connectés au réseau. Il s'agit, par exemple, des paquets envoyés ou reçus, des octets envoyés ou reçus, des erreurs et des paquets de broadcast et de multicast.
- **Groupe des systèmes hôtes TopN** – Génère un rapport des systèmes hôtes TOPN en s'appuyant sur les statistiques du groupe des systèmes hôtes.
- **Groupe des matrices de trafic** – Stocke les erreurs et les statistiques d'utilisation relatives aux paires de nœuds qui communiquent sur le réseau. Il s'agit, par exemple, des erreurs, des octets et des paquets.
- **Groupe des filtres** – Moteur de filtrage qui génère un flux de paquets à partir de trames correspondant au schéma défini par l'utilisateur.
- **Groupe d'interception des paquets** – Définit la méthode de mise en tampon interne des paquets qui répondent aux critères de filtrage.

- **Groupe des événements** – Permet de consigner des événements, également appelés pièges générés, à l'intention de l'administrateur, avec date et heure. Il s'agit par exemple de rapports personnalisés s'appuyant sur le type d'alarme.

Activité de média interactive

Associer: Activité de correspondance RMON

À la fin de ce TP, l'étudiant sera en mesure de comprendre les termes, les définitions et le fonctionnement de l'analyseur RMON.

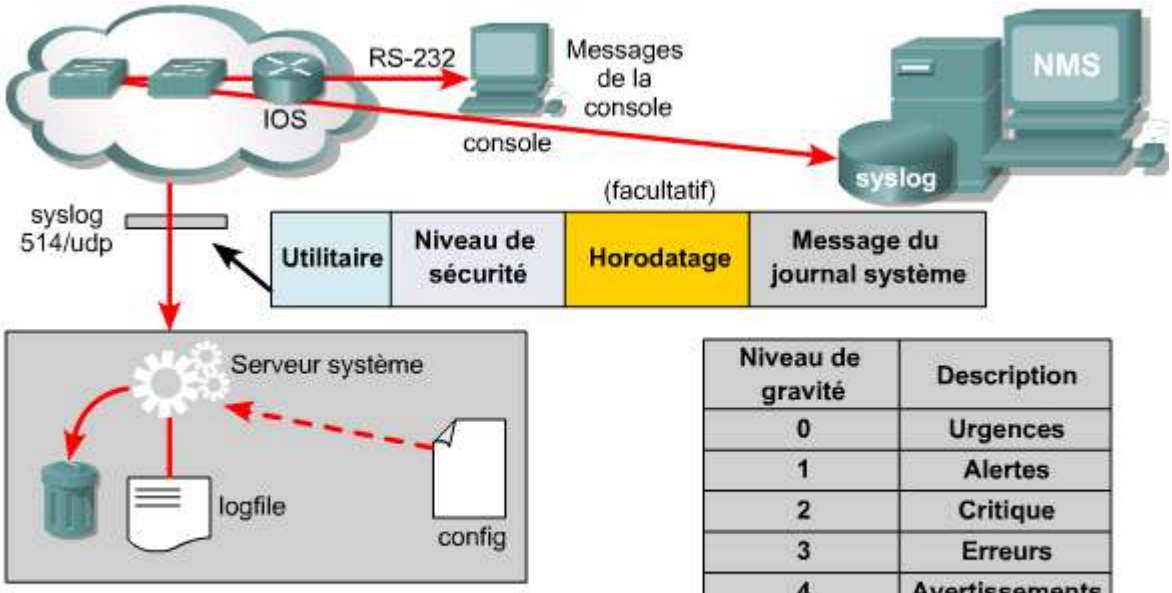
6.2 Administration réseau

6.2.9 Syslog

L'utilitaire de consignation Cisco syslog est fondé sur l'utilitaire UNIX syslog. Les événements système sont généralement consignés sur la console, sauf si la fonction est désactivée. L'utilitaire syslog est un mécanisme permettant aux applications, aux processus et aux systèmes d'exploitation d'équipements Cisco de rendre compte des activités et des conditions d'erreur. Le protocole syslog s'utilise pour permettre aux équipements Cisco d'envoyer ces messages non sollicités à une station d'administration réseau.

Chaque message syslog consigné est associé à un horodatage, une installation, une gravité et un message de consignation en texte. Ces messages sont parfois la seule manière d'obtenir des éclaircissements sur le dysfonctionnement d'un équipement.

Le niveau de gravité indique la nature cruciale du message d'erreur. 1



Niveau de gravité	Description
0	Urgences
1	Alertes
2	Critique
3	Erreurs
4	Avertissements
5	Notifications
6	Informatif
7	Débogage

Niveau par défaut de IOS Syslog →

Il existe huit niveaux de gravité, de 0 à 7, le niveau 0 (zéro) étant le plus critique et le niveau 7 le moins critique. Ces niveaux sont présentés ci-dessous:

0 Urgences

1 Alertes

2 Critique

3 Erreurs

4 Avertissements

5 Notifications

6 Informations

7 Débogage

Les champs de l'installation (facility) et du niveau de gravité (severity level) servent à traiter les messages. Les types de fonctions entre le niveau 0 (zéro) et le niveau 7 sont fournies pour le traitement des messages de consignation personnalisés. Par défaut, Cisco IOS adopte le niveau de gravité 6. Ce paramètre est configurable.

Pour que la NMS puisse recevoir et consigner les messages système d'un équipement, syslog doit être configuré sur ce dernier. 2

```
logging on
logging <hostname | IP_Addr>
logging facility local7
logging trap informational
logging source-interface loopback0
logging timestamps log datetime
```

Vous trouverez ci-dessous un récapitulatif de la syntaxe des commandes de configuration de ces équipements.

Pour activer la consignation sur toutes les destinations prises en charge:

```
Router(config)#logging on
```

Pour envoyer des messages de consignation du journal vers un hôte du serveur syslog, tel que CiscoWorks2000:

```
Router(config)#logging hostname | ip address
```

Pour définir le niveau de gravité sur 6 ou Informations:

```
Router(config)#logging trap informational
```

Pour inclure l'horodatage avec le message de syslog:

```
Router(config)#service timestamps log datetime
```

Résumé

La compréhension des points clés suivants devrait être acquise:

- Les fonctions d'une station de travail et d'un serveur
- Les rôles des divers équipements dans un environnement client/serveur
- Le développement de systèmes d'exploitation de réseau
- Une vue d'ensemble des diverses plates-formes Windows
- Une vue d'ensemble de certaines des alternatives aux systèmes d'exploitation Windows
- L'intérêt de l'administration réseau
- Les couches d'OSI et du modèle d'administration réseau
- Le type et l'application des outils d'administration réseau
- Le rôle de SNMP et de CMIP dans la surveillance réseau
- La manière dont les logiciels d'administration recueillent des informations et consignent les problèmes
- Les méthodes de collecte de rapports sur les performances réseau

- Une station de travail est un ordinateur client utilisé pour exécuter des applications. Elle est connectée à un serveur à partir duquel elle obtient des données partagées avec d'autres utilisateurs. Un serveur est un ordinateur qui exécute un système d'exploitation de réseau.
- Le modèle d'architecture client-serveur répartit la charge de traitement entre plusieurs ordinateurs.
- Un système d'exploitation de réseau autorise la communication entre plusieurs équipements et le partage de ressources sur l'ensemble d'un réseau.
- L'administration réseau se compose des activités suivantes :
  - Contrôle de la disponibilité du réseau
  - Automatisation améliorée
  - Contrôle des temps de réponse
  - Fonctions de sécurité
  - Réacheminement du trafic
  - Capacité de restauration
  - Enregistrement des utilisateurs
- L'organisme international de normalisation ISO (International Standards Organization) a créé un comité visant à produire un modèle pour l'administration des réseaux, sous la direction du groupe OSI. Ce modèle se décline en quatre parties : organisation, information, communication et fonctionnalité.
- Pour permettre l'interopérabilité de l'administration sur de nombreuses plates-formes réseau différentes, des normes d'administration s'avèrent nécessaires pour que les constructeurs puissent les mettre en œuvre et y adhérer. Deux normes principales ont émergé : SNMP (Simple Network Management Protocol) et CMIP (Common Management Information Protocol)
- SNMP est un protocole de couche application, conçu pour faciliter l'échange d'informations de management entre des équipements réseau.
- Une base d'informations de management (MIB) sert à stocker les informations structurées représentant les éléments du réseau et leurs attributs.
- L'utilitaire syslog est un mécanisme permettant aux applications, aux processus et au système d'exploitation des équipements Cisco de faire état des conditions d'erreur et d'activité.